

Data Migrator Administration Guide

Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS
Modules

VSP N series

Hitachi NAS Platform

Release 13.9

© 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, 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, the Microsoft Corporate 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 at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Preface	7
Related Documentation.....	7
Accessing product documentation.....	10
Getting help.....	10
Comments.....	10
Chapter 1: Overview of Data Migrator and Data Migrator to Cloud	12
Advantages of using Data Migrator.....	12
Data migration paths.....	13
Types of migration targets.....	13
Cross volume links in Data Migrator	14
Data Migrator licenses.....	15
Adding a license key.....	16
Chapter 2: Using Data Migrator.....	18
Configuring Data Migrator.....	18
Data Migrator considerations	19
Viewing data migration paths.....	22
Configuring Data Migrator paths.....	23
Adding a local WFS/HNAS data migration path.....	24
About external data migration paths.....	27
Viewing data migration rules.....	27
Adding a data migration rule by template.....	28
Adding a custom WFS/HNAS data migration rule.....	34
Modifying a data migration rule.....	35
Viewing data migration policies and schedules.....	36
Adding a WFS/HNAS data migration policy.....	38
Using Pre-Conditions.....	42
Modifying a data migration policy.....	43
About the ndmp-management-ports-set command.....	45
Migration schedules.....	45
Adding a Data Migration schedule.....	45
Modifying a schedule.....	47
Data Migration status and reports.....	48
Viewing details of a data migration report.....	49

Migration to HCP Systems.....	53
Chapter 3: Using Data Migrator to Cloud.....	56
Data Migrator to Cloud overview.....	56
Configuring Data Migrator to Cloud.....	56
Checking and setting the status of aggregate ports for Data Migrator to Cloud.....	57
Ensuring that the route exists when using aggregate ports.....	58
Ensuring the route exists when using management ports.....	58
Data Migrator to Cloud Configurations	58
Target on the Internet when using aggregate ports	59
Data Migrator to Cloud with aggregate support and target on LAN.....	59
About cloud accounts and destinations.....	60
Cloud providers.....	61
Using the Hitachi Content Platform cloud providers.....	63
Establishing credentials for Amazon S3.....	64
Establishing a Microsoft Azure cloud account.....	64
Establishing an S3 Cloud Object Storage account.....	65
Importing a web server certificate.....	65
Adding a cloud account.....	66
Adding a cloud destination.....	68
Viewing cloud accounts and destinations.....	68
Viewing Cloud Account Details.....	71
Viewing Cloud Destination Details.....	72
Viewing data migration paths.....	73
Adding a cloud path.....	74
Viewing data migration rules.....	75
Adding a data migration rule by template.....	76
Adding a data migration rule for the Data Migrator to Cloud.....	82
Modifying a data migration rule.....	83
Viewing data migration policies and schedules.....	84
Adding a cloud data migration policy.....	87
Using Pre-Conditions.....	90
Modifying a data migration policy.....	91
Migration schedules.....	93
Adding a Data Migration schedule.....	93
Modifying a schedule.....	94
Data Migration status and reports.....	95
Viewing details of a data migration cloud report.....	97
Cloud data migration and replication considerations.....	99
Introduction to HCP no delete feature.....	104
HCP no delete functionality.....	104

Chapter 4: Overview of Hitachi NAS Universal Migrator.....	107
Overview of Universal Migrator Capacity Based (UMC) license.....	107
Universal Migrator Capacity License considerations.....	108
Universal Migrator Capacity event notification.....	108
Hitachi NAS Universal Migrator Terms	108
Pre-migration considerations for Hitachi NAS Universal Migrator.....	109
Number and layout associations.....	109
NFS export on the LNAS used by HNAS.....	109
Export/shares from HNAS.....	110
Backup and replication policies, disaster recovery.....	110
Virtualization.....	110
Migration.....	110
HNAS NDMP file replication and tape backups.....	111
Setting up LNAS and HNAS for virtualization.....	112
Starting virtualization.....	113
Monitoring the association.....	114
Incompatible features.....	114
Performance Limitations.....	114
Upgrade and downgrade considerations.....	115
Troubleshooting Hitachi NAS Universal Migrator.....	115
Cannot create associations.....	115
Hitachi NAS Universal Migrator associations paused.....	115
Virtualization or migration does not complete.....	116
Hitachi NAS Universal Migrator Console Commands.....	116
virtualization-license-report CLI command.....	116
virtualization-path-control CLI command.....	116
virtualization-path-create CLI command.....	117
virtualization-path-delete CLI command.....	117
virtualization-path-excluded-directory-add CLI command.....	117
virtualization-path-excluded-directory-delete CLI command.....	117
virtualization-path-excluded-directory-list CLI command.....	117
virtualization-path-files CLI command.....	117
virtualization-path-journal-control CLI command.....	117
virtualization-path-journal-show CLI command.....	118
virtualization-path-list CLI command.....	118
virtualization-path-modify CLI command.....	118
virtualization-path-stats CLI command.....	118
Appendix A: Creating specific and detailed migration rules.....	119
Rules syntax.....	120
Keywords.....	121

Connectors.....	124
Conditionals.....	124
Statement order.....	125
Appendix B: Configuring management ports for Data Migrator to Cloud.....	127
Data Migrator to Cloud Environment Variables.....	130

Preface

This guide provides information about the Data Migrator feature, including how to set up migration policies and schedules. Note that some features apply only to individual platforms and may not be applicable to your configuration.

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](https://support.hitachivantara.com/en_us/contact-us.html) 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](https://community.hitachivantara.com) 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 us your comments on this document 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: Overview of Data Migrator and Data Migrator to Cloud

NAS Platforms support multiple storage technologies, with different performance capacity and cost characteristics.

In order to take full advantage of tiered storage, data should be organized using a tiered hierarchy of importance and need. Data Migrator makes it easier to move data among different tiers of storage.

Advantages of using Data Migrator

There are five key reasons to use Data Migrator with the server:

- 1. Cost-Efficient Storage Utilization:** Using Data Migrator, newer or routinely accessed data can be retained on primary storage, while older, less-accessed, or less performance-critical data is migrated to cost-efficient secondary storage. Data that has been migrated to secondary storage can be moved back to primary storage if it becomes active again.
- 2. Easy Policy-Based Configuration:** Data Migrator uses logical policies that invoke simple building blocks of rules to classify files as available for migration or reverse migration (returning the data from secondary storage to primary storage). Data Migrator rules and pre-conditions can include a file's size, type, access history, creation date, or owner, among other criteria. Files meeting the criteria in the rules and pre-conditions are migrated (or reverse migrated).
- 3. Discreet Migration:** Migrations are handled as automated background tasks with minimal impact on server performance. While migrations are in progress, all data can continue to be accessed normally.
- 4. Client Transparency:** Files migrated off primary storage are replaced by a link. The link looks and functions identically as the original file. When the link is accessed, the contents of the associated file are retrieved transparently from their location on secondary storage. To the client workstation, they appear indistinguishable. During a reverse migration, the data is moved from secondary to primary storage, and the link is removed.
- 5. Maximizing Storage Efficiency through Migration Reports:** Migration reports are created at the end of each migration cycle. These reports detail file usage and space consumption patterns, revealing opportunities to create more aggressive migration policies, freeing up more primary space.

Further migration possibilities can be gauged by scheduling Data Migrator test runs where reports can be produced without an actual migration taking place.

Data migration paths

Before any data migration is run, the location of the migration target must be defined by creating a data migration path. A data migration path is a long term relationship between a migration source, which can be a file system (for Data Migrator and Data Migrator to Cloud) or a virtual volume (for Data Migrator only) and a migration target, which may be a local file system, a set of file systems, a remote location, or a list of locations. Once a migration path has been used, it cannot be deleted until files migrated through that path have been deleted.

The advantages of having this long term relationship between a migration source and a target are as follows:

1. Other system software can stop file systems from being destroyed when they are actively used by a migration path. This avoids migrated files becoming inaccessible.
2. Where snapshots can be taken on the target (local Data Migrator only), synchronized source and target snapshots can be taken to maintain snapshot images of migrated files.
3. When recovering from tape or replicating a file system that included migrated data, data which was originally migrated can be placed back on the migration target.

If using virtual volumes individually as migration sources within migration paths, the file system containing the virtual volumes cannot be used as a migration source itself. Currently, it is only possible to define one migration path for a given migration source.

Types of migration targets

Data Migrator can move data to secondary storage attached directly to the storage server/cluster (a local migration), or to secondary storage attached to an external server that is not connected to the storage server/cluster (a remote migration).



Note: Performing a remote migration from one Enterprise Virtual Server (EVS) in a cluster to another EVS in the same cluster is not supported. The reason for this restriction is that it would be dangerous to configure migration from one EVS of a cluster to another EVS on the same cluster. The danger arises because, in the case of a failure of the destination (target) EVS, that failed EVS could fail over to the same node as the migration's source EVS, which would cause all the migrated files to become inaccessible.

Local migrations provide the benefits described previously, and remote migrations extend the functionality of Data Migrator to allow storage administrators to free up local storage resources by migrating data to storage attached to a remote NFSv3 server or a cloud target such as Hitachi Content Platform (HCP). Data may also be migrated to a remote server for a variety of other reasons, including archival, deduplication, or policy-based retention, compliance, and access control. As with files migrated locally, when a client tries to read a file migrated to a remote server, the file is retrieved and sent to the client, so there is no indication to the client that the file is not in their local file system.



Note: A single migration path or operation can be made between local targets or remote targets, but not both local and remote targets.

Remote migrations are controlled by user defined policies, just like the policies created for local migrations. Only the paths to the secondary storage are different. Local migrations have paths to secondary storage that is attached to the same server/cluster that hosts the primary file system, while remote migrations have external paths (the secondary storage is attached to a remote server).



Note: A remote migration to a Hitachi Content Platform (HCP) or to a cloud target uses the HTTP/HTTPS protocol. A remote migration to any other remote server uses the NFS protocol.

Cross volume links in Data Migrator

Data Migrator allows you to move data from primary to secondary storage based on policies that you define. When a file is migrated, a cross volume link is left, indicating the new location of the file's data. A cross volume link is a special file on the local file system that "points" to the file on a remote file system. The cross volume link stores the migrated file's metadata and is used to construct a handle for the file on the remote file system.

When a read request for a migrated file is received, the storage server reads the cross volume link, constructs the file handle, retrieves the file from the secondary storage, and sends the file to satisfy the read request. In this way, the read request is serviced and the client need not be aware that the file is not actually stored on the local file system.

Enhanced cross volume links (CVL-2) are supported on all NAS Platforms and offer the following benefits:

- Remote file systems might be on a storage device attached to a remote server (not necessarily another NAS Platform) accessible through the NFSv3 protocol. This capability, called remote migration, allows the storage server to migrate files to a separate storage device, such as content archival or compliance products.

Remote migration to a Hitachi Content Platform (HCP) system, is supported through the HTTP or HTTPS (cloud only) protocol for new remote migration paths, but pre-existing remote migration paths that were created in releases that supported the NFSv3 protocol are still supported. You cannot, however, create paths to an HCP system using the NFSv3 protocol.

Access to files located on the external storage device is a licensed feature, requiring an external volume link (XVL) license and a Data Migrator license. See the *Server and Cluster Administration Guide* for information on adding a license key.

- Local access to migrated file attributes increases performance for getattr/lookup/readdir+ requests.

For enhanced cross volume links (CVL-2), all file attributes for a migrated file are stored on the local file system. When an operation requires the attributes of a migrated file, the storage server responds with locally stored attribute information, which provides better performance.

In addition, local read caching can be used to improve performance when accessing migrated files. See the *Server and Cluster Administration Guide* for information on local read caching.

- Quota management and CVL-2 links.

File-size-based quotas consider the size of a file to be its logical length (the length shown by 'ls -l') and as such ignore the fact that files may resize on an external location.

Usage-based quotas compute the size of a file from the number of local blocks that it currently uses. A file which has been externally migrated uses zero local (non-metadata) blocks, so will appear to a usage-based quota to be of size zero.

Data Migrator licenses

In order to use Data Migrator, you need a license.

The following licenses are available for this feature:

- **DM** - this license is required for classic Data Migrator and also for Data Migrator to Cloud. It permits data migration to internal targets.
- **XVL** - this license is required for external data migration, that is, external cross volume links which are outside of an EVS. This license permits data migration to NFS servers and supported cloud providers, for example, HCP.

Adding a license key

Adding a license key can enable services or increase the capabilities of your system. To add a license key:

Procedure

1. Navigate to **Home > Server Settings > License Keys**.
2. Click **add**.

The following table describes the fields on this page:

Field/Item	Description
Add a File License Key	
File License Key	Enables the user to manually enter the license key.
Import File License Keys From a File	
File License Key File Name	Enables the user to import a license key from a file.
Import Block License Keys From a File (NAS module only)	
Block License Key File Name	Enables the user to import a software application license key from a file.
cancel	Closes the page without saving configuration changes.



Note: After adding a license key, if a reboot is required in order to start a service/protocol or enable a feature, you are instructed to reboot or restart the system.

For a file license, you can either enter the key manually or import it from a file. For a block license, you can only import the key from a file:

- To enter the key manually, type it in the field, then click **add**.
- To import the key, click **Choose File / Browse**, navigate to the file, select the key file, then click **Import**.

After all the keys have been entered or imported, they will be displayed on the **License Keys** page. Follow the instructions to reboot the system (if necessary).

Chapter 2: Using Data Migrator

This chapter describes the Data Migrator features and provides instructions on how to add paths, rules, policies, and schedules.

If you are using Data Migrator to Cloud, refer to the next chapter.

Configuring Data Migrator

To use Data Migrator, you must define the following:

- Data migration paths from primary to secondary storage.

Data migration paths define the relationship between primary and secondary storage. The primary and secondary storage defined in the data migration paths must be assigned to the same EVS.

- Data migration rules, which define the properties of files that will be migrated.
- Data migration policies, which define rules to apply to specific data migration paths based on the available free space on the source file system or dynamic file volume.

Free space is calculated as follows:

- For a file system, free space is the amount of unused space allocated to the file system (before it automatically expands, if automatic expansion is enabled for the file system).
 - For a virtual volume, if a quota has been defined, free space is the amount of unused space before reaching the usage limit of the quota for that virtual volume. If a quota has not been defined for the virtual volume, free space is the same as the free space for the file system.
- Schedules, which define when data migration policies are run and files are migrated.

Data Migrator considerations

The server uses Data Migrator with the following considerations:

- **Snapshots and local migrations:** If files are migrated locally (to storage attached to the same EVS), when snapshots are created on the primary file system, corresponding snapshots are automatically created on the secondary file system. This preserves snapshot protection on migrated files. Likewise, when a snapshot is deleted on the primary file system, the corresponding snapshot on the secondary file system is automatically deleted.

When attempting to access a locally migrated file through a snapshot on primary storage, the server will look for the corresponding snapshot on secondary storage and retrieve the migrated data from that snapshot. If the secondary file system does not contain any snapshots, the file contents will be retrieved from the live file system.

- **Snapshots and remote migrations:** If files are migrated to storage attached to a different server (a remote migration), when snapshots are created on the primary file system, corresponding snapshots are not created on the secondary file system.

To preserve snapshot protection on migrated files for remote migrations, you must ensure that snapshots are taken of the storage attached to the remote server. Snapshots on the secondary file system are not managed, used, or accessed by the storage server.

When a snapshot is accessed, and the snapshot contains a file system with a cross volume link, no special processing of the cross volume link is performed if the file in the snapshot is equivalent to the live file. If the file in the live file system has been modified since the snapshot was taken (if it differs from the file in the snapshot), attributes from the file in the snapshot are returned for `getattr/lookup/readdir+` requests, but an error is returned for read requests.

- **Virtual volume:** If files are migrated locally, either enhanced cross volume links or original cross volume links may be used depending on your configuration. When files are migrated to a remote server, enhanced cross volume links are always used.
 - **If enhanced cross volume links are used**, virtual volumes are not recreated at all on the secondary storage.
 - **If original cross volume links are used**, virtual volumes that are present on primary storage, will be automatically recreated on the secondary storage when the data is moved during the first scheduled run of the data migration policy.
- **Quota space tracking:** Quotas are enforced only on the file system or virtual volume on which they were created. When a file is migrated through Data Migrator, however, the contents are moved from one file system to another file system or virtual volume, which may be on a remote server. Cross volume links are used to link the data from its original location to its new location. Quota tracking is different based upon the type of cross volume link being used:
 - **When enhanced cross volume links are used**, and files are migrated to a file system on a remote server, quotas are tracked just as if the file had remained in its original location. Quotas are tracked entirely on the local file system because file space and file count quotas are managed and calculated using local attributes. This behavior simplifies quota management but does not allow storage administrators to set up separate quotas for data based on the data's location.
 - **When original cross volume links are used**, and files are migrated to another file system or virtual volume on the same server/cluster, quotas on primary storage are only effective on files that have not been migrated. To track space utilization of migrated data, quotas must be manually defined on secondary storage. Quota restrictions on virtual volumes cannot be set until after the policy has been completed.

- **Backup, restore, and replication of migrated files:**When backing up a migrated file, NDMP will backup the entire contents of the file by retrieving it from secondary storage. Additionally, the backed up file will be identified as having been a migrated file. In this way, if the file is restored to a file system or virtual volume that has been configured as primary storage in a data migration path, the contents of the file will automatically be restored to secondary storage, leaving a cross volume link on the primary storage. If the restore target is not part of a data migration path, the file will be restored in its entirety.

Alternatively, the NDMP environment variable `NDMP_BLUEARC_EXCLUDE_MIGRATED` can be used to prevent migrated data from being backed up. This can also be useful if the effective data migration policies are configured to migrate non-critical files such as music and video files from home directories or aged data. It can also improve backup and replication time, and isolate the backup data set to include only the critical information on primary storage.

You can back up a file system that is the target of a data migration. This is accomplished by performing backup of the primary file system, and selecting an option to back up only the files that have been migrated to the secondary file system. This functionality is controlled via the `NDMP_BLUEARC_INCLUDE_ONLY_MIGRATED` NDMP environmental variable, which does the opposite of the `NDMP_BLUEARC_EXCLUDE_MIGRATED`. See the *Backup Administration Guide* for more information.

It is important to remember that Data Migrator extends the maximum available capacity of primary storage by migrating data to secondary storage. This means that the capacity of the backup solution, whether tape library or a replication target, must also support the new maximum available capacity. To maintain a reliable backup and recovery system, ensure that the capacity of the deployed backup solution is at least equal to the combined capacity of primary and secondary storage. Alternatively, use `NDMP_BLUEARC_EXCLUDE_MIGRATED` to isolate the backup dataset to only those files that are hosted natively on primary storage.

Replication of migrated files:If a file has been migrated from primary storage, and a replication operation attempts to copy the file, NDMP can be set to:

- **Ignore migrated files:**If set to ignore, the replication operation copies only the files on the primary storage (migrated files are not copied).
- **Recreate links to migrated files:**If set to recreate links, the replication operation copies only the details of the cross volume link. The cross volume link is recreated on the destination if the relevant external migration data path is in place and the migrated file is accessible.
- **Remigrate migrated files:** (the default) If set to remigrate, the replication operation copies the file contents but marks the file as having been externally migrated. The destination re-migrates to secondary storage if there is an existing data migration path.

This functionality is controlled using the NDMP environment variable `NDMP_BLUEARC_EXTERNAL_LINKS`. See the *Backup Administration Guide* for more information.

- **Files with hard links:**Files with hard links are migrated.
 - The first instance of a hard link matching the criteria will be migrated and stubbed. This results in all other hard links to be immediately considered as stubs so that redundant migration does not occur. The last instance of the stubbed hard link on the file system to be deleted will cause the object to be deleted on the target.
- **Migrated file access:**Files that have been migrated should not be accessed directly by clients on the secondary file system. All access to migrated files should be done through the primary storage server.

Viewing data migration paths

You can view the data migration paths in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Data Migration Paths**.

The screenshot shows the 'Data Migration Paths' page in the NAS Manager. The breadcrumb navigation is 'Storage Management > Home > Storage Management > Data Migration Paths'. The main heading is 'Data Migration Paths'. Below it is a table with the following columns: Primary File System, Primary Virtual Volume, Secondary Target Type, Secondary File System(s), EVS, Status, and a 'details' button. There are two rows of data. The first row has 'HDS' for Primary File System, 'None' for Primary Virtual Volume, 'Cloud' for Secondary Target Type, 'CLI-hcp-encrypt-default' for Secondary File System(s), 'mercury10-s' for EVS, and 'OK (no links exist)' for Status. The second row has 'HDS' for Primary File System, 'None' for Primary Virtual Volume, 'WFS/HNAS' for Secondary Target Type, 'None (Test Only)' for Secondary File System(s), 'mercury10-s' for EVS, and 'OK (unused)' for Status. Below the table are links for 'Check All' and 'Clear All'. Underneath the table are action buttons: 'Add WFS/HNAS Path', 'Add Cloud Path', and 'delete'. At the bottom, there are shortcuts: 'Policies and Schedules', 'Data Migration Rules', and 'Data Migration Cloud Accounts'.

Primary File System	Primary Virtual Volume	Secondary Target Type	Secondary File System(s)	EVS	Status	
<input type="checkbox"/> HDS	None	Cloud	CLI-hcp-encrypt-default	mercury10-s	OK (no links exist)	details
<input type="checkbox"/> HDS	None	WFS/HNAS	None (Test Only)	mercury10-s	OK (unused)	details

Check All | Clear All

Actions: [Add WFS/HNAS Path](#) [Add Cloud Path](#) [delete](#)

Shortcuts: [Policies and Schedules](#) [Data Migration Rules](#) [Data Migration Cloud Accounts](#)

The following table describes the fields on this page:

Field/Item	Description
Primary File System	The file system from which data will be migrated.
Primary Virtual Volume	If a virtual volume has been selected as primary storage, this field displays the name of the virtual volume from which data will be migrated.
Secondary Target Type	Destination target to which the data will be migrated.
Secondary File Systems	Displays the secondary file system.
EVS	The EVS hosting the file system from which data will be migrated.
Status	Status of the data migration path. The status should always be OK; if otherwise, migrated files might be inaccessible.
details	Displays the details of the selected data migration path.
Add WFS/HNAS Path	Displays the Add WFS/HNAS Path page.
Add Cloud Path	Displays the Add Cloud Path page.
delete	Deletes the specified migration policy.
Policies and Schedules	Displays the Data Migration page.
Data Migration Rules	Displays the Data Migration Rules page.
Data Migration Cloud Accounts	Displays the Cloud Accounts and Destinations page.

Configuring Data Migrator paths

There are different types of paths between primary and secondary storage.

- **Primary storage** (typically Fibre Channel disk arrays) is the source for data migrations.
- **Secondary storage** (typically SATA disk arrays) is the target for data migrations. Note that there are two types of paths to secondary storage:
 - **Local paths** - these are paths to secondary storage attached to the same EVS, storage server, or cluster. Local paths can be added using the NAS Manager.
 - **External Paths** - these are paths to secondary storage that is attached to a remote server (a NAS Platform, or another server using the NFS protocol, or a Hitachi Content Platform using the HTTP protocol). External paths cannot be added using the NAS Manager. Instead, you must use CLI commands.

After Data Migrator has been configured, data is migrated from primary to secondary storage based on the data migration rules and schedules, freeing up space and extending the capacity of the primary storage.

Caution: *Dysfunctional backups alert!* Accessing files directly on secondary storage might alter access and modification times of the files, resulting in unexpected results when performing backups. The organizational structure of migrated data on secondary storage does not mirror that of primary storage.

Caution: *Lost access to migrated files alert!* If only the primary or only the secondary file system is moved to a different EVS, access to migrated files will be lost. If both the primary and the secondary file systems are moved to the same EVS, access to migrated files will be retained. When moving file systems, File System Relocation is the recommended method, because, when using File System Relocation, if the file system being moved is a member of a data migration path, both the data migration source file system and the target file system are relocated. See the *File Services Administration Guide* for more information.

Caution: *Exclusive migration pathing!* Once a migration path has been assigned to a virtual volume, a subsequent migration path cannot be created to its hosting file system. Also, once a migration path has been assigned to a file system, subsequent migration paths cannot be created from virtual volumes hosted by that file system.

Note: When defining data migration paths, specify a file system or virtual volume as the primary storage. Once a file system is selected as primary storage, that entire file system, including all virtual volumes is included as a part of the data migration policy. Therefore, in order to create individual policies for different parts of a file system, create virtual volumes and assign each virtual volume a unique migration path.

Adding a local WFS/HNAS data migration path

You can add a data migration path in the NAS Manager.



Procedure

1. Navigate to **Home > Storage Management > Data Migration Paths**.
2. Click **Add WFS/HNAS Path**.

The screenshot shows the 'Add WFS/HNAS Path' configuration window. The breadcrumb navigation is 'Storage Management > Home > Storage Management > Data Migration Paths > Add WFS/HNAS Path'. The window title is 'Add WFS/HNAS Path'. The 'Primary' section has 'EVS / File System' set to 'g1-evs1 / FS_1' with a 'change...' button, and 'Virtual Volume' set to 'testVvol' with a dropdown arrow. The 'Secondary' section has instructions: 'Select secondary WFS/HNAS file system(s) to which data will be migrated. In most circumstances, only one file system should be selected.' Below this are two columns: 'Available' and 'Selected'. The 'Available' column contains a list box with 'None (Test Only)', 'SourceFS', and 'vmdastore'. The 'Selected' column is empty. At the bottom are 'OK' and 'cancel' buttons.

The following table describes the fields on this page:

Section	Item/Field	Description
Primary	EVS/File System	The EVS and file system of the primary storage. This defines the source of the data migration path. To change the currently selected EVS and file system, click change....
	Virtual Volume	By default, data migration policies include the entire file system. To configure migrations on a per virtual volume basis, fill this check box and select the virtual volume to be used as the primary storage for this data migration path.
Secondary	Available	File systems to which the data will be migrated (the destination file system). Select the destination file system from the list. The file systems you select should be on secondary storage.

Section	Item/Field	Description
		<p> Note: When creating a policy for testing purposes, select "None (Test Only)." Running this policy will then determine the outcome of the migration operation without actually moving data.</p> <p>In most cases you should specify a single destination file system to create a "single-target" migration path. However, if the amount of data is too large for a single target file system, you may want to nominate multiple file systems as targets to create a "multi-target" migration path.</p> <p>For "multi-target" migration paths, you should be aware of the following:</p> <ul style="list-style-type: none"> ■ Data is distributed between the destination file systems based on the amount of free space available on those file systems. If the destination file system is expandable, the data distribution algorithm calculates free space not based on the file system's current size, but on the maximum size to which a file system can be expanded. ■ Once specified, multi-target paths may not be modified through NAS Manager. If you need to change the migration path targets, for instance to add an additional destination file system, you must use the migration-expand-target command through the CLI. <p> Note: We can add a path for an internal migration through NAS Manager. For external migrations, use the following CLI command: <pre>migration-add-external path -s Source_File_Name -n Logic_Name -t nfs://EVS-IP_Target/ Export_Name_Target.</pre></p>
	Selected	The file systems selected to be the destination of the migration.

3. Select the primary file system or virtual volume whose data will be migrated to a file system in secondary storage. Ensure that both the primary and secondary data belong to the same EVS.

4. Verify your settings, then click **OK** to save or **cancel** to decline.

About external data migration paths

External data migration paths are not defined through NAS Manager. Instead, CLI commands are used to specify the path to external secondary storage. These commands are:

- `migration-add-external-path`
- `migration-change-external-path`
- `migration-delete-external-path`
- `migration-expand-external-path`

For information about these commands, refer to the *Command Line Reference*, or the man page for each command.

You should specify a unique external path for each file system being migrated to a remote server.

After an external migration path has been defined, it will be visible and available for selection in the NAS Manager **Data Migration Paths** page.



Note: Do not define an external migration path from one EVS in a cluster to another EVS in the same cluster. The reason for this restriction is that it would be dangerous to try to migrate from one EVS of a cluster to another EVS of the same cluster. If the destination (target) EVS fails during the migration, it could fail over to the same node as the source EVS, which would cause all the migrated files to become inaccessible.

After the external migration path has been configured using the CLI, all remaining external migration management tasks may be performed through NAS Manager, including specifying migration policies, rules, and schedules.



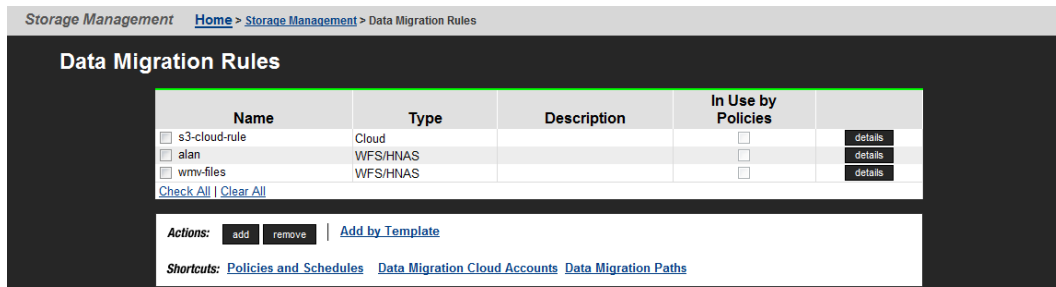
Note: When adding external migration paths, make sure that the remote server's IP address or host name is correct and, if using a host name, make sure that the host name is resolvable (fully qualified domain names are also acceptable).

Viewing data migration rules

The **Data Migration Rules** page lists all existing rules and provides for editing or removal of selected rules and creation of new rules.


Data migration rules are used in conjunction with data migration paths to form data migration policies.

Navigate to Home>Storage Management>Data Migration Rules to display the **Data Migration Rules** page.



The following table describes the fields on this page:

Item/Field	Description
Name	The name given when the rule is created. It is used to identify the rule when creating or configuring policies.
Type	The type of data migration that this rule can be used for.
Description	A description of the rule to help identify the criteria to be applied.
In Use by Policies	The check box is filled when a rule is being used by one or more policies.
details	Click for a selected migration rule to display its complete details.
add	Click to create custom rules that will define the criteria by which the files will be migrated.
remove	Click to remove one or more existing rules.
Add by Template	Click to create simple rules using predefined templates.
Policies and Schedules	Goes to the Data Migration Policies and Schedules page. New policies and schedules can be created there.
Data Migration Cloud Accounts	Goes to the Cloud Accounts and Destinations page. New cloud accounts and destinations can be created there.
Data Migration Paths	Goes to the Data Migration Paths page. New paths can be created there.

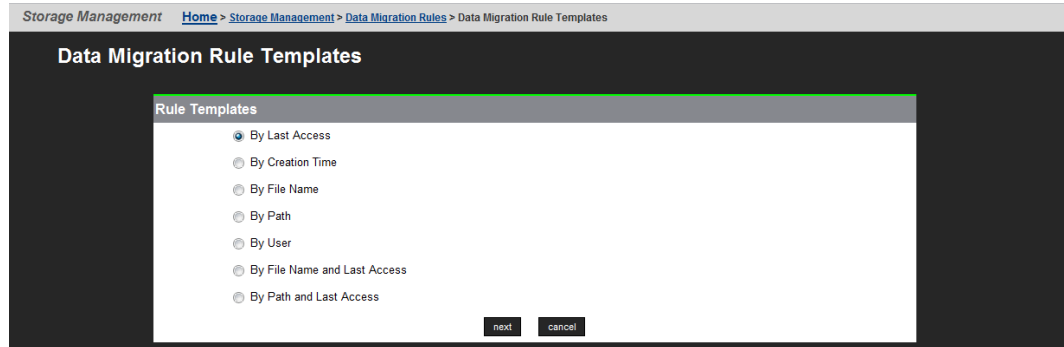
 **Caution:** Once created, do not change a data migration rule without verifying that it is not used by existing policies, as such changes might result in unintentional changes to existing policies.

Adding a data migration rule by template

Rules define the properties of files that will be migrated.


Procedure

1. To create rules that suit more specific migration needs, navigate to **Home > Storage Management > Data Migration Rules** to display the **Data Migration Rules** page, and then click **Add by Template** to display the **Data Migration Rule Templates** page:



2. Select a **Rule Template**, then click **next**.
The following table describes each of the available rule templates:

Rule Template	Description
By Last Access	Migrates all files that have remained inactive (or have been active) within a certain period of time.
By Creation Time	Migrates all files created before or after a specific point in time.
By File Name	Migrates all files with the same name and extension. An asterisk can be used as a wildcard character. For example: <ul style="list-style-type: none"> ▪ <code>dbfile.db</code> migrates all files with the name <code>dbfile</code> and the extension <code>.db</code>. ▪ <code>*.db</code> migrates any file with an extension of <code>.db</code> regardless of the file name. ▪ <code>dbfile.*</code> migrates all files with the name <code>dbfile</code> and any extension.

Rule Template	Description
	<ul style="list-style-type: none"> *dbfile.db migrates all files ending with the name dbfile and the extension .db. dbfile* migrates all files with a name beginning with dbfile and having any extension.
By Path	Migrates all files under a particular directory.
By User	Migrates all files of the specified users. <div style="border: 1px solid black; background-color: #e0f2f1; padding: 5px; margin-top: 10px;">  Note: This rule does not apply to the Data Migrator to Cloud. </div>
By File Name and Last Access	Migrates files of a certain name and/or extension (as described above) that have remained inactive for a certain period of time.
By Path and Last Access	Migrates all files under a certain directory that have remained inactive for a certain period of time.

3. Enter requested template-specific information:

- If you select **By Last Access**, the **Data Migration Rule: Last Access Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Include Criteria	To specify the maximum period a file can be inactive before being migrated to a secondary file system: <ol style="list-style-type: none"> a. From the menu, select inactive. The menu includes an option for selecting the opposite scenario; that is, to choose active within to specify files that have been active within the specified period. b. From the menu, select the period (days, hours, or minutes). c. Enter the threshold quantity period.

- If you select **By Creation Time**, the **Data Migration Rule: Creation Time Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Include Criteria	To specify the point in time for the migration rule: <ol style="list-style-type: none"> From the first menu, select more than or less than. Enter the threshold number. From the second menu, select month(s), week(s), day(s), hour(s), or minute(s).

- If you select **By File Name**, the **Data Migration Rule: File Name Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Include Criteria	To specify the type of files (based on their file extension) to be migrated to a secondary file system: <ol style="list-style-type: none"> From the menu, select include. The menu also has an option for selecting the opposite scenario; that is, selecting to exclude files not of the specified type. In the all files named field, enter the file name and extension. More than one file name or extension can be named in this field separated by commas; for instance: *.jpg, *.bmp, *.zip.

- If you select **By Path**, the **Data Migration Rule: Path Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Include Criteria	To specify the path to the files under a certain directory: <ol style="list-style-type: none"> From the menu, select include. The menu also has an option for selecting the opposite scenario; that is, to select exclude to select all files that are not in the path. In the all files in the path field, enter the directory file path.

- If you select **By User**, the **Data Migration Rule: User Name Template** page contains the fields described in the following table:



Note: This option only applies to WFS/HNAS and does not apply to Data Migrator to Cloud.

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	You can only enable the WFS/HNAS option. This rule does not apply to cloud options.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Include Criteria	To specify the user names for the owners of the files to be migrated to a secondary file system: <ol style="list-style-type: none"> From the menu, select include. The menu also has an option for selecting the opposite scenario; that is, selecting to exclude files from owners other than the specified owners.

Item/Field	Description
	<p>b. In the all files in the path field, enter the UNIX or Windows user names for the owners of the files you want to migrate. More than one user name can be listed in this field, but names must be separated by commas. For instance, <code>jjames, myco\smithr, myco\smith</code>.</p> <p>Windows user names are specified in the form <code>domain\user name</code>, and backslashes in user names should not be escaped (double backslashes are not required).</p>

- If you select **By File Name and Last Access**, the **Data Migration Rule : Last Access Time and File Name Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, fill this check box.
Include Criteria	<p>To migrate inactive files from a specified directory to a secondary file system:</p> <ul style="list-style-type: none"> a. In the All files named field, enter the file name extension of the files to be migrated. For example <code>note.txt</code>, <code>note*</code>, or <code>mp3</code>. b. In the All files not accessed within___ field, enter the threshold quantity. c. Select the period from the list. You can choose days, hours, or minutes.

- If you select **By Path and Last Access**, the **Data Migration Rule: Last Access Time and Path Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, fill this check box.
Include Criteria	To migrate inactive files from a specified directory to a secondary file system: <ol style="list-style-type: none"> In the All files in the Path field, enter the directory file path. In the All files not accessed within___ field, enter the threshold quantity. Select the period from the list. You can choose days, hours, or minutes.

4. Verify your settings, then click **OK** to save or **cancel** to decline.

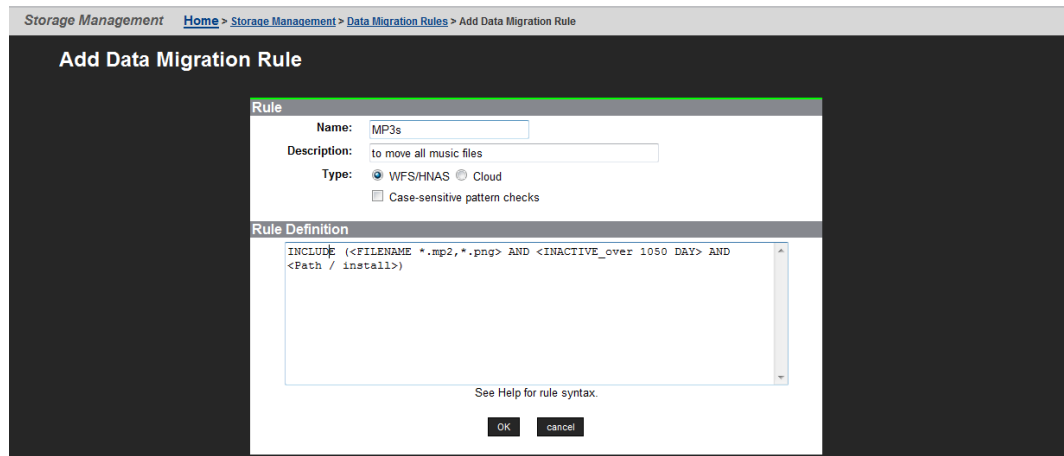
Adding a custom WFS/HNAS data migration rule

Use the **Add Data Migration Rule** page to name, define, and add data migration rules using rule syntax. Rules can be built with a series of INCLUDE and EXCLUDE statements. Each of these statements can contain a number of expressions specifying the type of files and the conditions under which they will be migrated.

For example: `INCLUDE (<FILENAME * .mp3> AND <FILE_SIZE_OVER 2GB>)`

Procedure

1. Navigate to **Home > Storage Management > Data Migration Rules** and then click **add** to display the **Add Data Migration Rule** page:



The following table describes the fields in this page.

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	Click the WFS/HNAS or Cloud option, as appropriate.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Rule Definition	Insert the syntax for the data migration rule.

2. Verify your settings, then click **OK** to save the rule, or click **cancel** to decline.

Modifying a data migration rule

You can modify a data migration rule in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Data Migration Rules**.
2. Select the check box next to the rule to modify and then click **details**.
The following table describes the fields on this page:

Field/Item	Description
Name	Displays the name of the rule.
Description	The description of the rule. Make any changes as appropriate.
In Use by Policies	Displays any associated policies in use for this policy. If none are used, displays 'Not in use.'
Type	Displays the type of rule, either Cloud or WFS/HNAS.
Case-sensitive pattern checks	Select the check box if the rule checking must be case sensitive.
Rule Definition	Displays the current definition in use. Modify if necessary.

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

Viewing data migration policies and schedules

Having created both data migration paths and data migration rules, data migration policies can now be created. Policies assign a rule or set of rules to a specific data migration path. They also define the conditions that initiate data migrations.

Procedure

1. To view data migration policies, navigate to **Home > Storage Management > Data Migration** to display a list of policies and schedules.

The screenshot shows the 'Data Migration' page in a web interface. It contains two main sections: 'Policies' and 'Schedules'.

Policies Table:

Name	EVS	Primary File System	Secondary File System	Rule	
<input type="checkbox"/> CloudMigration1	mercury10-s	HDS	CLI-hcp-encrypt-default	s3-cloud-rule	details

[Check All](#) | [Clear All](#)

Actions: [add](#) [remove](#)

Shortcuts: [Data Migration Rules](#) [Data Migration Cloud Accounts](#) [Data Migration Paths](#) [NDMP Configuration](#)

Schedules Table:


Policy Name / Schedule ID	EVS	Next Run	Migration Type	Last Status	
<input type="checkbox"/> CloudMigration1 / 5	mercury10-s	2014-05-30 00:00:00 (UTC-0700)	Migrate files (daily)	No Status	details

[Check All](#) | [Clear All](#)

Actions: [add](#) [remove](#) [run now](#) [Stop Migration\(s\)](#)

Shortcuts: [Data Migration Status & Reports](#)

The following tables describe the fields on this page:

Item/Field for Policies	Description
Name	Name of a data migration policy.
EVS	Primary EVS from which the migration originates.
Primary File System	Files in the primary file system or virtual volume that will be migrated.
Secondary File System	Secondary file system, to which all data will be migrated to.  Note: If the path to the secondary file system is an external path, the name or IP address of the server hosting the secondary file system is also displayed in parentheses. The displayed server name/IP address is a link, and you can click the link to display the full path.
Rule	Rules that can be triggered in this migration policy.
details	Displays the details for the selected policy.
add	Advances to the Add Data Migration Policy page.
remove	Deletes the selected migration policy.
Data Migration Rules	Advances to a page where all the configured data migration rules will be displayed. New rules can be created here as well.
Data Migration Cloud Accounts	Advances to the Cloud Accounts and Destinations page.
Data Migration Paths	Displays the configured data migration paths. New paths can be created as well.
NDMP Configuration	Advances to a page where the NDMP can be configured by entering the username, password, and NDMP version number.

Item/Field for Schedules	Description
Policy Name/Schedule ID	Displays the name given to the Data Migration Policy
EVS	Displays the primary EVS from where the migration is scheduled to originate.
Next Run	Displays the month, date, year and time for the next scheduled data migration run for this policy.

Item/Field for Schedules	Description
Migration Type	Displays the type of data migration that has been scheduled to run: <ul style="list-style-type: none"> ▪ Migrate files (followed by only once, daily, or weekly depending on the selected scheduled type). ▪ Simulate migration - Generates a one-time report of files that would be migrated. Does not actually migrate files. ▪ Report migrated files - Generates a one-time report with a list of previously migrated files. This migration type only applies to WFS/HNAS and not Data Migrator to Cloud.
Last Status	Displays the final status of the last run of the data migration operation.
details	Displays the current settings for the selected schedule.
add	Advances to the Add Data Migration Schedule page.
remove	Deletes the selected migration policy.
run now	Starts the scheduled data migration immediately.
Stop Migration(s)	Click the Stop Migrations link to stop a selected, in-process migration. Only migrations in progress can be stopped.
Data Migration Status & Reports	Advances to a page where all the completed migration runs will be listed in detail.

Adding a WFS/HNAS data migration policy

You can add a WFS/HNAS data migration policy in the NAS Manager.

Procedure

1. Navigate to and then click **add** under the Policies section to display the **Add Data Migration Policy** page.

The following table describes the fields in this page:

Item	Description
Policy Identification	This section allows you to specify a name to identify the migration policy.
Name	Name for the new data migration policy.
Migration Path	This section allows you to specify the data migration path to be used by the migration (or reverse migration) policy.
Migrate Data	When creating a migration policy, this section displays the data migration source and target information: <ul style="list-style-type: none"> ▪ Primary EVS/File System: Displays the name of the EVS and file system for primary storage (the migration source). ▪ Virtual Volumes: If a virtual volume has been selected as primary storage, the virtual volume will be displayed.

Item	Description
	<ul style="list-style-type: none"> ▪ Secondary Target Type: Displays WFS/HNAS to represent the migration type. ▪ Secondary File System: Displays the name of the file system on secondary storage that will host the migrated data (the migration target).
Reverse Migrate	When creating a reverse migration policy, this section displays the destination for the reverse migration (the original data migration source and target information). Files that have been migrated from the original source to secondary storage will be returned to this EVS and File System when the reverse migration policy criteria are met.
change...	Opens the Select a Path page, which enables you to select a different path.
Data Migration Paths	Opens the Data Migration Paths page, which allows you to create data migration paths.
Pre-Conditions	This section allows you to specify the rules (the criteria) that the files must match/meet in order to be migrated (or reverse migrated) according to this policy.
Available WFS/HNAS Rules	<p>Rules with specific threshold limits are displayed here. This list of rules define the set of conditions which trigger the migration/reverse migration. You can:</p> <ul style="list-style-type: none"> ▪ Add a Pre-condition to the Selected Rules list by selecting it and clicking the right arrow (>). ▪ Remove a rule from the Selected Rules list by selecting it and clicking the left arrow (<). <p>This policy will be run either by a defined schedule, or when started manually. Once the policy is run, the threshold specifies when the selected rules are applied. You can specify that the selected rules will be applied when either of the following conditions are met:</p> <ul style="list-style-type: none"> ▪ When the primary file system's free space falls below X% (set the percentage level for the condition). ▪ When other conditions are not met. These conditions are defined in the selected rule(s). <p>After selecting rules and the threshold, save the policy by clicking OK.</p>
Selected WFS/HNAS Rules	Displays the rules containing the criteria/conditions to be used to determine if a file should be migrated. The criteria in the rules are applied when the threshold (the when condition specified in the Available Rules section) is met.

Item	Description
Data Migration Rules	Opens the Data Migration Rules page, which allows you to create rules.

- Add a descriptive name for the policy. The name should make it easy to recognize the purpose of the policy.
- Select a migration path. You can specify that the policy:
 - Migrate Data:** To move the data from the primary file system to the secondary file system when the criteria defined in the Selected Rules are met.
 - Reverse Migrate:** To move the data from the secondary file system back to the primary file system when the criteria defined in the Selected Rules are met.
- Select one of the migration paths you created on the Data Migration Paths page. The path specifies the source and the destination of the migration. For a:
 - Migration operation, the source is the primary file system and the destination is the secondary file system.
 - Reverse migration operation, the source is any secondary file system and the destination of the reverse migration is the primary file system (the original source).

When a file is migrated, a CVL (cross volume link) or an XVL (external volume link) is left in the primary file system to point to the file in the secondary file system.

If the currently displayed path is not the one you want this policy to use, click **change** to display the **Select a Path** page:

Primary File System	Primary Virtual Volume	Secondary Target Type	Secondary File System(s)	EVS	Status
<input type="radio"/> HDS	None	Cloud	CLL-hcp-encrypt-default	mercury10-s	OK (no links exist)
<input type="radio"/> HDS	None	WFS/HNAS	None (Test Only)	mercury10-s	OK (unused)

OK cancel

(For more Primary/Secondary options, see [Data Migration Paths](#))

Select the path you want the policy to use, then click **OK**.



Note: If you are adding a policy to perform a test migration, a valid migration path is required, but it may be a real path involving primary and secondary file systems, or a “test-only” path in which a secondary file system does not exist.

- Select the rules and specify when the rules will be applied. Using the **Pre-conditions** section, specify the rules that contain the criteria that must be met in order to migrate the file. Also, choose the threshold that triggers the migration of the file.
- Verify your settings, then click **OK** to save the policy as defined, or **cancel** to return to the **Data Migration** page.

Using Pre-Conditions

When a migration policy is scheduled to run, it evaluates the percentage of available free space in the Policy's primary storage. Based on this analysis, one rule may be triggered to define the data set subject to migration. Migrations of data from primary storage then occurs based on the statements in the rule that was triggered. Only a single rule will be engaged during any particular migration operation.

When defining pre-conditions, customer support recommends aggressive tiering; specifically, it may be desirable to migrate .mp3 files and the contents of the directory /tmp regardless of the available free space. Then, if free space on primary storage is reduced to less than 50%, also to migrate all files not accessed within the last sixty days. Finally, if available free space is reduced to less than 15%, also to migrate the contents of users' home directories.

The following rules illustrate this scenario:

Rule	Statement
Rule 1:	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>
Rule 2:	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>
	INCLUDE (<INACTIVE_OVER 60>)
Rule 3:	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>
	INCLUDE (<INACTIVE_OVER 60>)
	INCLUDE (<PATH /home/*>)

Related pre-conditions

- Rule 3 if free space is less than 15%.
- Rule 2 if free space is less than 50%.
- Rule 1 if no other condition applies.

When the migration policy is scheduled to run, different rules may be triggered based on the available free space on primary storage. When a migration policy is engaged, only a single rule will be triggered to run.

For example:

- If free space is at 80%, then Rule 1 will be used.
- If free space is at 40%, then Rule 2 will be used.
- If free space is at 10%, then Rule 3 will be used.

When percentage thresholds are specified, they are evaluated based on whole number percentages. This means that if two rules are specified, one that will take effect at 8% of free space and one at 9% of free space, if the file system has 8.5% free space available, then the rule with the 8% pre-condition will apply.



Note: If the primary storage defined in the migration path is a virtual volume, free space will be based on the limit defined by the virtual volume quota. If this quota has not been defined, then free space available will be based on the free space of the file system hosting the virtual volume.

Connection Errors

When attempting to add a new migration policy, a connection error may be indicated by a message saying "Unable to connect to <IP address>" or "Error accessing <source/destination> server".

The "Unable to connect to" message means one of the following:

- The server is not currently powered up or is temporarily disconnected from the network. The server must be available and properly connected when creating a migration policy.
- The NDMP service may be disabled. The migration uses the NDMP service which must be enabled when adding or running replications. Use the NDMP configuration page (or the `ndmp-status` command) to enable and start the NDMP service.
- The Gigabit Ethernet port providing access to the EVS which hosts the File System is not accessible from the SMU. This may be the case if the network is set up with private subnetworks as commonly used with VLANs. In this case, the server may have been configured so that SMU access is through the management ports instead of the ports set using the `ndmp-management-ports-set` command.

The "Error accessing server" message may occur as a result of restricting NDMP access using the `ndmp-option` command. The `allowip` and `blockip` options can be set such that the SMU is not allowed to access the NDMP services via the standard routes. If the NDMP connection restrictions are definitely required, change the configuration of the server to allow SMU access via the management ports using the `ndmp-management-ports-set` command. The SMU connections then bypass the `allowip/blockip` checks.

Modifying a data migration policy

You can modify a data migration policy in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Data Migration**.
2. Select the policy to modify and then click **details** to display the **Modify Data Migration Policy** page.

The following table describes the fields:

Item	Description
Policy Identification	Name of the data migration policy.
Migration Path	The specified data migration path to be used by the migration (or reverse migration) policy.
Pre-Conditions	This section allows you to modify the rules (the criteria) that the files must match/meet in order to be migrated (or reverse migrated) according to this policy.
Available Rules	<p>Rules with specific threshold limits are displayed here. This list of rules define the set of conditions which trigger the migration/reverse migration. You can:</p> <ul style="list-style-type: none"> ▪ Add a Pre-condition to the Selected Rules list by selecting it and clicking the right arrow (>). ▪ Remove a rule from the Selected Rules list by selecting it and clicking the left arrow (<). <p>This policy will be run either according to a defined schedule, or when started manually. Once the policy is run, the threshold specifies when the selected rules are applied. You can specify that the selected rules will be applied when either of the following conditions are met:</p> <ul style="list-style-type: none"> ▪ When the primary file systems free space falls below X% (set the percentage level for the condition). ▪ When other conditions are not met. These conditions are defined in the selected rule(s). <p>After selecting rules and the threshold, save the policy by clicking OK.</p>
Selected Rules	Displays the rules containing the criteria/conditions to be used to determine if a file should be migrated. The criteria in the rules are applied when the threshold (when condition specified in the Available Rules section) is met.
(To create rules, see Data Migration Rules)	Advances to the Data Migration Rules page, which allows you to create rules.

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

About the `ndmp-management-ports-set` command

The NAS Manager replication and data migration features use the NDMP service on the NAS server. The NDMP service is usually accessed via the IP address of the EVS which hosts the file system, this access usually happens through a Gigabit Ethernet port. In some cases, the IP address is within a private subnetwork and is not accessible from the NAS Manager. When this is the case, the `ndmp-management-ports-set` command can be used to request that the NAS Manager access goes through the management ports and is then relayed to the NDMP service.

The `ndmp-management-ports-set` command takes two parameters which are the TCP ports. One is used to accept the incoming connection on the management port and one is used to pass the requests to the NDMP code. These must be ports that are not in use by any other service. In particular, these ports must not be the standard NDMP service port. The port numbers 10001 and 10002 usually work and, being next to the standard NDMP port 10000, can be useful in identifying the port usage.

Having set up the NDMP management ports this way, all NAS Manager replication and data migration NDMP accesses will be routed via the management port. Note that the actual data transfer connections involved are between the NAS server EVSs and do not run over the management connections. In particular, a replication between two NAS servers passes the data over a TCP connection between EVS IP addresses through the Gigabit Ethernet ports. Therefore, the two EVSs must have IP addresses that can communicate with each other.

Migration schedules

After a data migration policy has been defined, it must be scheduled. The decision on how often to run a policy may be affected by the rules selected in this policy. For example:

- A policy with a single rule to migrate all `.mp3` files may be scheduled to run once every month.
- Another policy, used to archive a working `/project` directory once the project is complete, may be scheduled as a Once Only Schedule.
- Other policies which migrate based on various Pre-conditions, and are triggered on available free space, may be scheduled to run every week.

When planning migration schedules, schedule migrations during off-peak times, such as evenings and weekends.

After a data migration has begun, additional data migrations for the same policy cannot be started until the current one has completed. However, it is possible to start multiple concurrent data migrations if each have its own policy.

Adding a Data Migration schedule

You can add a data migration schedule in the NAS Manager.



Note: You must create a migration policy before you can schedule a migration.

Procedure

1. Navigate to **Home > Storage Management > Data Migration**.

- Click **add** in the Schedule section of the page to display the **Add Data Migration Schedule** page:

The following table describes the fields on this page:

Field/Item	Description
Data Migration Policy	Select a migration policy from the list.
Migration Type	Choose from the following migration type options: Migrate Files: Select this option and then choose only once, daily, or weekly, from the list. Selecting the Once Only option causes the policy to run only once, at the specified date and time. Simulate Migration: Select this option to generate a report of files that would be migrated. Does not actually migrate files. Only run once. Report Migrated Files: Select this option to generate a report with a list of previously migrated files. Only run once. This option only applies to WFS/HNAS and does not apply to Data Migrator to Cloud.
Date and Time to Start	Specifies when the policy will run. From the calendar next to the field, select the start date for the policy's initial run. The selected date appears on the field.

Field/Item	Description
	Enter the scheduled run time in a 24 hour setting (for example, 11:59 PM will be entered as 23:59). The current NAS Manager date and time are provided below for reference.
Duration Type	Choose from the following duration types: Run until migration completes indicates that the scheduled policy should run until it has completed. Suspend migration after x Hours:Minutes. Resume when the next schedule starts indicates the scheduled policy should be suspended after the time specified and resumed at the next scheduled interval. Note that this option only applies to Data Migrator to Cloud and not to WFS/HNAS.

3. Verify your settings. Then click **OK** to save or **cancel** to decline.

Modifying a schedule

Once defined, schedules can be easily modified to meet the changing requirements of data migration policies. When modifying a schedule, the scheduled date and time, as well as the interval in which the schedule will run can be changed.

Procedure

1. Navigate to **Home > Storage Management > Data Migration**.
2. Under the Schedules section of the page, fill the check box next to the schedule to modify and then click **details**.

The following table describes the fields on this page:

Field/Item	Description
Data Modify Policy	Name of the schedule. This is a read-only field.
Data Migration Type	The type of migration: WFS/HNAS, External, or Cloud.
Migration Type	Displays the current option. Migrate files - options are: <ul style="list-style-type: none"> ▪ only once ▪ daily ▪ weekly Simulate Migration - Generates a report of files that would be migrated. Does not actually migrate files. Only run once.

Field/Item	Description
	Report Migrated Files - Generates a report with a list of previously migrated files. Only run once. This option applies to WFS/HNAS and External data migration types and does not apply to Data Migrator to Cloud type.
Next Run	Date and time of next scheduled run.
Initial Run	Date and time of initial run.
Reschedule	To change this, fill in the check box and enter the new date and time.
Duration Type	<ul style="list-style-type: none"> ▪ Run until job completes indicates that the scheduled policy should run until it has completed ▪ Suspend migration after x Hours:Minutes. Resume when the next schedule starts indicates the scheduled policy should be suspended after the time specified and resume at the next scheduled interval. Note that this option only applies to the Data Migrator to Cloud.

3. Make any modifications as necessary.
4. Click **OK**.

Data Migration status and reports

After a data migration policy has completed a cycle, it generates a data migration report that includes details about files migrated, including available free space before and after the migration. Reports of the last five scheduled migrations are routinely saved; the rest are purged. If a schedule is deleted, so are its reports.

Migration reports can be downloaded in CSV format, then imported into a spreadsheet and processed, saved, or printed. These reports are useful when studying the system access patterns, file storage tendencies, the efficiency of rules, paths, policies and schedules. By gauging file and space usage statistics of Primary and secondary storage, Data Migrator reports can be used to refine a rule or pre-condition. The more precise and aggressive the rule, the better Data Migrator serves the storage system.

To view a list of existing reports, navigate to Home>Storage Management>Data Migration Status & Reports.

Storage Management [Home](#) > [Storage Management](#) > Data Migration Status & Reports

Data Migration Status & Reports

Display Options
 Group by Policy Name [refresh](#)

Show: 20 Items per page

Schedule Id	Server	EVS	Policy	Completed	Files Migrated	Status
1	g1-cluster	g1-ers3	MPS	2014-05-29 16:20:43 (UTC-0700)	0	OK

Actions: [remove](#) [Remove All](#)

Shortcuts: [Policies and Schedules](#)

The following table describes the fields on this page:

Item	Description
Display options: Group by policy name	Selecting this option groups the data migrations by policy name, even if they are sorted in a different order, for example, the completed time and date.
Schedule ID	ID number for the completed migration.
Server	Primary file system's server.
EVS	Primary file system's EVS.
Policy	Policy name.
Completed	Year, month, day and time when the migration was completed.
Files Migrated	Number of files that were migrated.
Status	Migration completion status.
details	Opens the Data Migration Report page where you can view the details of the select report.
remove	Click to remove a selected report.
Remove All	Click to remove all migration reports in the list.
Policies and Schedules	Opens the Policies and Schedules page where you can view, add, and remove existing policies and schedules.

Viewing details of a data migration report

To view data migration reports, navigate to Home > Storage Management > Data Migration Status & Reports, and then click details to display the **Data Migration Report** page:

Storage Management [Home](#) > [Storage Management](#) > [Data Migration Status & Reports](#) > Data Migration Report

Data Migration Report

Report Summary

<p>Migration Policy: MPS Schedule ID: 1 Status: OK View Log Migration Type: Migrate files Frequency: Daily</p>	<p>Start Time: 2014-05-29 16:20:43 (UTC-0700) End Time: 2014-05-29 16:20:43 (UTC-0700) Duration: 00:00:00</p>
<p>Server / EVS: g1-cluster / g1-eva3 Rule Used: None Amount Migrated: 0 Bytes Files Migrated: 0 Files Failed: 0</p>	

PHDS1 - Primary File System Statistics

Pre-Migration File System Space Used			Post-Migration File System Space Used			File System Capacity	Live File System Reclaimed	Total File System Reclaimed
Live FS	Snapshots	Total Usage	Live FS	Snapshots	Total Usage			
3.90 GiB (1%)	0 Bytes (0%)	3.90 GiB (1%)	3.90 GiB (1%)	0 Bytes (0%)	3.90 GiB (1%)	500.75 GiB	0 Bytes (0%)	0 Bytes (0%)

Actions: [back](#) [delete](#) | [View Log](#) [Download Migration Report](#)

The following table describes the contents of this page:

Item	Description
Report Summary	
Migration Policy	Completed migration policy name.
Schedule ID	Migration schedule ID.
Status	Migration completion status. If the status is OK , the migration completed successfully. If the status is Error , the migration is not complete.
Migration Type	Type of migration, migrate files, simulate migration, report migrated files.
Frequency	How often the Policy is scheduled to run.
Start Time	Date and time when the migration began.
End Time	Date and time when the migration ended.
Duration	Duration of migration.
Server/EVS	EVS on which the Primary and secondary storage reside.
Rule Used	Rule used by the policy.
Amount Migrated	The migrated amount of data.
Files Migrated	Quantity of files that were migrated. If files have been migrated, click this to view a list of the files that were migrated. The list provides details on their path, size, and their start and end times.
Files Failed	Number of files that should have been migrated but were not. For example, files in use at the time of the migration may not be migrated.
Primary File System Statistics	
Pre-Migration File System Space Used	File system size, snapshot size, and the total used space before the migration.
Post-Migration File System Space Used	File system size, snapshot size, and the total used space after the migration.
File System Capacity	File system's total capacity.
Live File System Reclaimed	Reclaimed space in the live file system, defined as the usable space on the file system; that is, the part of the file system not reserved or in use by snapshots.

Item	Description
Total File System Reclaimed	Reclaimed space in the total file system, defined as the entire capacity of the file system and includes usable space and space that is reserved or in use by snapshots.
Primary Virtual Volume Statistics	
Pre-Migration Virtual Volume Space Used	Details the virtual volume's size and the total space used before the migration.
Post-Migration Virtual Volume Space Used	Details the virtual volume's size and the total space used after the migration.
Virtual Volume Reclaimed	Displays the virtual volume space gained due to the migration.
Secondary File System Statistics	
Pre-Migration File System Space Used	File system size, snapshot size, and the total used space before the migration.
Post-Migration File System Space Used	File system size, snapshot size, and the total used space after the migration.
File System Capacity	File system's total capacity.
Live File System Reclaimed	Space taken up due to the migration.
Total File System Reclaimed	Total space used in the file system by migration.
Secondary Virtual Volume Statistics	
Pre-Migration Virtual Volume Space Used	Details the virtual volume size and the total space used before the migration.
Post-Migration Virtual Volume Space Used	Details the virtual volume size and the total space used after the migration.
Virtual Volume Consumed	Displays the virtual volume space taken up by the migration.
back	Returns to the previous page
delete	Permanently deletes the report

Item	Description
Download Migration Report	Downloads the report onto the local PC in a compressed format.

The following Actions are available:

- Click View Log to view a log file containing time, duration and status details of the migration. A View Log link is available at both the top and bottom of the page.
- Click Download Migration Report to view a report about the completed data migrations with details on the primary and secondary file systems and virtual volumes, including status, space utilization before and after the migration, the duration, start, and end time for the migrations.

Included in the download are two other important reports: one that lists all the files that were migrated (list.gz) and the other that lists all the files that were not migrated (failed.gz).

Migration to HCP Systems

The Hitachi NAS Platform supports migration of data to Hitachi Content Platform (HCP). After a file has been migrated, when a network client attempts to change the read-only attribute of a file that has been migrated to HCP, that request fails.



Note: Migration to HCP requires an external volume link (XVL) license and a Data Migrator license. See the Server and Cluster Administration Guide for information on adding license keys.

When Data Migrator migrates files to HCP systems, the HTTP protocol is used. Note the following:

- The storage server only supports migration to HCP systems via HTTP without SSL security.
- The only supported HTTP targets are HCP systems (migration to other remote servers uses the NFS protocol).
- The storage server does not support the use of an HTTP proxy to access the remote HCP system.

Functionality exists which enables the user to specify a list of files to be migrated to HCP. This is disabled by default. To enable this functionality, contact your support provider.

If this functionality is enabled then the list of files, called a migration request file, is placed into a migration control directory (specified as part of the migration path for the file system or virtual volume). The migration control directory is periodically checked by the NAS Manager. When a migration request file is found, a migration operation is started. Upon completion, a report file is created in the migration control directory. External migration paths must be set up before the migration control file is created and put into the migration control directory.

Reclaimed Space

Reclaimed space is the difference in available space between the start and completion of the migration. It is not a report of the amount of data migrated from the source file system to the target. For this information, refer to Amount Migrated.

It is likely that the file system will be in use by network clients while the migration is in progress. As a result, the reclaimed space can be substantially different than the amount migrated. The value can even be negative if files were added to the source.

Once a data migration has completed, copies of the files may be preserved on the source file system in snapshots. For the space to be fully reclaimed, all snapshots on the source file system that reference the migrated files must be deleted.



Note: When a reverse migration takes place, space on the primary file system is consumed as files are moved from the secondary file system back to the primary file system. Space in the secondary file system, however, is reclaimed.

Reversing Migration

The server does include support for automatic policy-based reverse migration of files as a part of the Data Migrator feature. Aside from the policy-based reverse migration, there are two ways you can manually cause migrated files to be restored to primary storage:

- **Reverse Migration Through the server CLI.** Individual files or whole directory trees can be reverse-migrated through the CLI. The files which are included in the reverse migration can be identified by pattern or by last access time. For detailed information on this process, run `man reverse-migrate` at the CLI.
- **Reverse Migration From a Network Client.** A file can be restored from a network client by performing the following sequence of operations:
 - From a Windows or Unix client, make a copy of the file (using a temporary file name) on the primary storage. This copy of the file will reside fully on primary storage.
 - Delete the original file. This will delete the link on primary storage, and the migrated data from secondary storage.
 - Rename the copied file to its original name.

iSCSI Logical Units

Mounted iSCSI LUs cannot be migrated, regardless what has been defined in the data migration policy. Due to the types of applications typically hosted on iSCSI storage, Hitachi Vantara Support Center does not recommend migrating iSCSI LUs to secondary storage. However, if this is desired, it can be accomplished by performing the following:

- Disconnect any iSCSI Initiators with connections to an LU.
- Unmount the iSCSI LU. This can be done through the iSCSI Logical Unit Properties page.
- Run the data migration policy to migrate the LU.

- Re-mount the iSCSI LU.
- Reconnect the Initiator to the iSCSI Target.

Chapter 3: Using Data Migrator to Cloud

! **Important:** It is important to read through this chapter even if you have experience with Data Migrator and are new to Data Migrator to Cloud.

Data Migrator to Cloud allows files hosted on the server to be moved or migrated to cloud storage, providing the benefits associated with both local and cloud storage. This feature makes it seamless to move data between different tiers of the storage.

Data Migrator to Cloud overview

Data Migrator to Cloud supports both public and private clouds.

A storage cloud is a pool of cost-effective, elastic, persistent storage accessible through some variant of the HTTPS protocol that provides reasonable access performance for uploading and downloading archived files. Combining Cross-Volume Link (CVL-2) technology with cloud storage provides a near seamless archiving experience.

A public cloud is provided by external entities hosting storage at their facility and paid for on a per-use basis. A private cloud is purchased and controlled by the end user.

With Data Migrator to Cloud, you can access the cloud storage directly to view and download data, and by accessing the files through the file system. In both scenarios data is protected both in-flight and at-rest regardless of where the physical storage is hosted.

Data Migrator to Cloud is similar in look and feel to Data Migrator whereby you must configure paths, rules, policies, and schedules for a file system. Data Migrator to Cloud also introduces the concepts of an account whereby the you enter credentials for the cloud target, and a destination, which is the location on the cloud in which the archived files are to be placed.

A license is required to use the Data Migrator to Cloud for non-HCP targets. Contact customer support to purchase a license.

Configuring Data Migrator to Cloud

To use Data Migrator to Cloud, you must define the following:

- An established network route. See the *Network Administration Guide* for details.
- Cloud account.
- Cloud destination.

- Cloud path, which defines the relationship between primary storage and to the cloud destination to which data will be migrated.
- Data migration rules, which define the properties of files that will be migrated.
- Data migration policies, which define rules to apply to specific data migration paths based on the available free space on the source file system. Free space is the amount of unused space allocated to the file system (before it automatically expands, if automatic expansion is enabled for the file system).
- Data migration schedules, which define when data migration policies are run.



Note: Data Migrator to Cloud is supported with the Virtual Secure Servers feature provided that the following two requirements are met:

1. A cloud target is resolvable in a DNS server configured in Global Context.
2. A route from the aggregate ports to the Cloud provider (Amazon S3, Microsoft Azure, S3 Cloud Object Storage or HCP) server exists on all nodes.



Note: For late-breaking Data Migrator to Cloud information, refer to the Release Notes.

Checking and setting the status of aggregate ports for Data Migrator to Cloud

In most cases, the default configuration of the ports should be sufficient and you will not need to take any action. To check the current data transfer mode that Cloud Gateway is running, issue the following CLI command:

migration-cloud-service-mode-show

- If this is the first time you are using Data Migrator to Cloud, the system will send data through the aggregate ports with zero copy for the local HCP cloud target.
- If you currently have Data Migrator to Cloud configured and running, the default will continue to be management ports. You have the option to switch and send data through the aggregate ports. If you decide to use aggregate ports, you must first ensure that the route exists. Once you confirm that the route exists, issue one of the following CLI commands:
 - **migration-cloud-service-mode-set -a** to transfer data through the aggregate ports.
 - **migration-cloud-service-mode-set -z** to transfer data at a higher outgoing performance rate through the aggregate ports for local HCP target servers.

For more information on the CLI commands, see the *Command Line Reference*

Tagged VLANs are supported with Data Migrator to Cloud. For information on VLANs, link aggregations, and adding aggregations, see the *Network Administration Guide*.



Note: Multi-tenancy is currently not supported when using network aggregates.

Ensuring that the route exists when using aggregate ports

To check the existence of a viable route from the EVS hosting the file system to the cloud server you want to migrate files to.

Procedure

1. Open a BALI command prompt window.
2. Enter `ping -I <source address> <target name>`
where `<source address>` is one of the IP addresses on the EVS associated with the file system and `<target name>` is the fully qualified domain name of the HCP namespace or cloud provider address.
3. The verification process is complete when the system successfully receives responses to the ping messages from the target. The following is an example of a successful ping to check cloud server reachability from an EVS, with the response of "0% packet loss."

```
mercury15:$ ping -I 192.168.43.22
ns01.tenant01.hcp01.us.dev.bluearc.com
ns01.tenant01.hcp01.us.dev.bluearc.com (10.23.34.58) ...
64 bytes from 10.23.34.58: icmp_seq=0 time=1 ms
64 bytes from 10.23.34.58: icmp_seq=1 time <1 ms
64 bytes from 10.23.34.58: icmp_seq=2 time <1 ms
64 bytes from 10.23.34.58: icmp_seq=3 time <1 ms
--
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0/0/1 ms
mercury15:$
```

4. If the route does not exist, refer to the *Network Administration Guide*.

Ensuring the route exists when using management ports

To check the existence of a viable route from the EVS hosting the file system to the cloud server you want to migrate files to.

Procedure

1. Open a Linux command prompt
2. Enter `ping <target name>`
where `<target name>` is the fully qualified domain name of the HCP namespace or cloud provider address.
3. If the route does not exist, refer to the *Network Administration Guide*.

Data Migrator to Cloud Configurations

Two example aggregate port configurations are presented in this section:

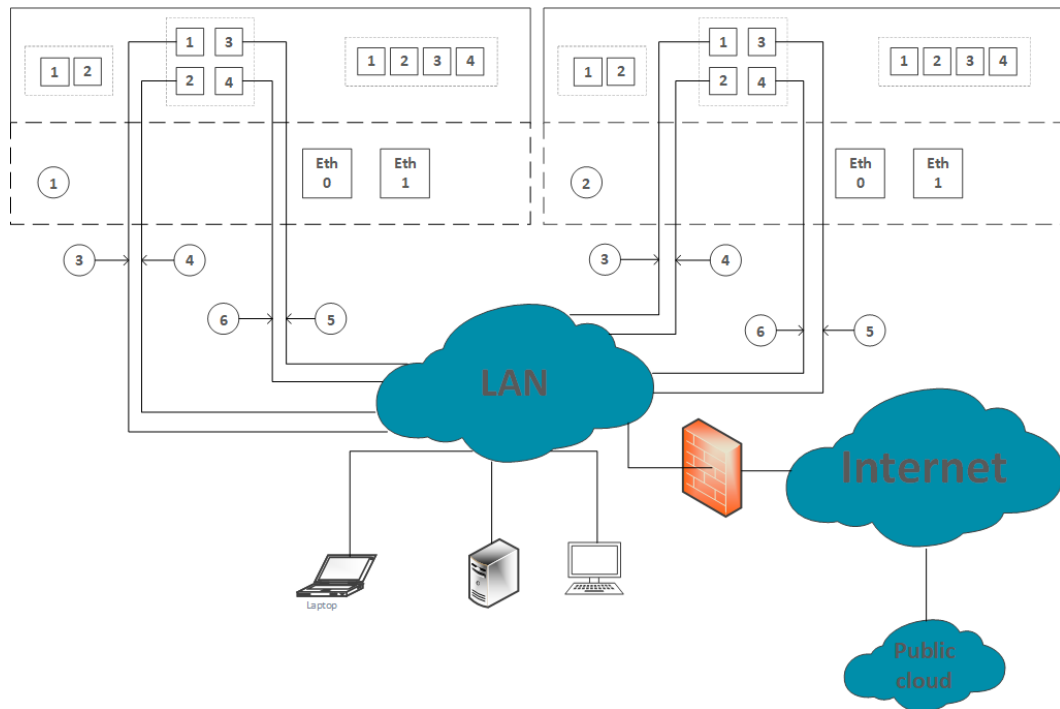
- Target on the Internet when using aggregate ports
- Data Migrator to Cloud with aggregate support with the target on the LAN

For all targets, the server must be able to resolve the hostname. Because the target is on the Internet, at least one of the configured DNS servers must be connected to the Internet.

For information on VLAN support, see the *Network Administration Guide*.

Target on the Internet when using aggregate ports

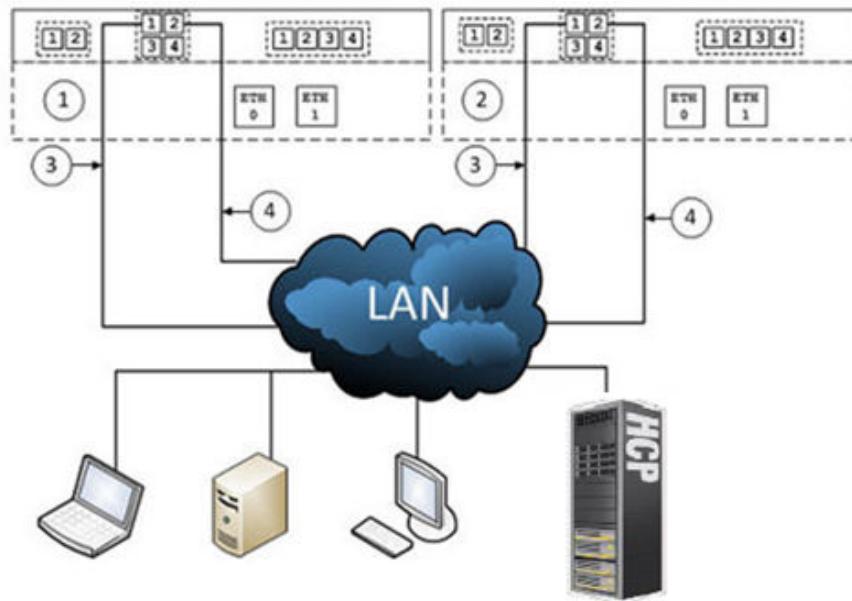
The server must be able to resolve the hostname *using one of the aggregate ports*. Because the target is on the Internet, at least one of the configured DNS servers must be connected to the Internet.



Item	Description
1	node 1
2	node 2
3	agg_1
4	agg_2
5	agg_3
6	agg_4

Data Migrator to Cloud with aggregate support and target on LAN

For this configuration, HNAS must be able to reach a DNS server using aggregate ports, which resolves the names of the target.



Item	Description
1	node 1
2	node 2
3	agg_1
4	agg_2

About cloud accounts and destinations

To use Data Migrator to Cloud, you must first configure at least one account that contains the following information:

- The cloud provider, currently either Hitachi Content Platform (HCP), Hitachi Content Platform (HCP S3), Amazon S3, S3 Cloud Object Storage or Microsoft Azure.
- The credentials of a user with read/write permissions to the target.
- A destination, which is a location on the cloud where migrated files will be stored. This destination must exist before using Data Migrator to Cloud. The configuration of the destination will fail if the specific destination cannot be validated.

Multiple accounts are supported. Also, note that multiple file system migration policies can use the same account.

Cloud providers

Data Migrator to Cloud supports multiple cloud providers.

The table below lists each cloud provider and the required information when adding a cloud account and destination.

Cloud Account					
Provider	Server Name	Destination Location	User Credentials	Server Credentials	References
HCP	Fully qualified domain name of the HCP namespace for the account credentials	The folder path. This field can be empty.	User name of the Data Access Account	The password of the Data Access Account with read/write/delete/purge/search permissions to the user account	
HCP (S3)	Fully qualified domain name of the HCP namespace for the account credentials	The folder path. This field can be empty.	User name of the Data Access Account	The password of the Data Access Account with read/write/delete/purge/search permissions to the user account	
Amazon S3	Auto-populates with aws-amazon.com	The bucket with or without a subfolder.	Access key	Security Credential Key	https://console.aws.amazon.com/iam/
Microsoft Azure	Auto-populates with azure.microsoft.com	The bucket with or without a subfolder.	Name of storage account	Primary or Secondary Access Key	https://azure.microsoft.com
S3 Cloud Object Storage	User must provide an endpoint name (for IBM see https://ibm-public-cos.github.io/crs-docs/endpoints)	The bucket with or without a subfolder.	Access key	Security Credential Key	for IBM see https://control.softlayer.com/

Using the Hitachi Content Platform cloud providers

The NAS server provides two types of Hitachi cloud provider.

The options are:

- Hitachi Content Platform
- Hitachi Content Platform S3

To ensure optimal configuration, check that:

- the account contains the fully qualified domain name of the HCP namespace. For HCP S3, the namespace must also have an assigned owner.
- the user permissions are sufficient. The required Data Access Permissions are for the tenant-level user include Read, Write, Delete, Purge, and Search for the given namespace. Tenant or system administrator privileges are not needed.
- HTTPS protocol is enabled
- the HTTP protocol is enabled if (for better performance) encryption-in-transit is not desired
- the default retention class is disabled

In addition to user permissions and retention class, there are extra attributes to set on an HCP S3 server:

- the tenant-level user needs an additional 'Privileged' Data Access Permission
- the tenant-level user must be the owner of the namespace
- ACL needs to be enabled
- HCP S3 Authenticated access requires the installation of HCP client certificates and HS3 API to be enabled
- the 'optimization for cloud protocols only' setting needs to be enabled
- MAPI, the Management API needs to be enabled for the tenant

Selecting a Hitachi Content Platform cloud provider

Use HCP S3 if:

- You are using S node storage, especially if you are using encryption or compression.
- You are using HCP version 8 or higher

Use HCP if:

- HCP is not configured to store data on S Node Storage
- HTTP protocol is used to leverage zero copy feature
- You are using HCP versions earlier than 8

The main difference between the two providers is the method used for file uploads and downloads:

A Hitachi Content Platform server can store data on S Series storage in both encrypted and un-encrypted formats. When the NAS server requests an encrypted (or compressed) file from S series storage through HCP, it makes HTTP ranged GET requests in 500KB chunks. In order to decompress or decrypt large files, HCP has to read the entire file multiple times. This can impact performance.

The **HCP S3** cloud provider uses multi-part upload functionality. This means that each chunk of data is encrypted and stored separately on the S series storage. When the NAS server requests an encrypted or compressed file, HCP only needs to retrieve the relevant chunks. This option increases performance when using encryption or compression on HCP S series storage with Data Migrator to Cloud.

You can select a provider when creating a new cloud account in the NAS Manager. Alternatively, if you already have a Hitachi Content Platform cloud provider configured, you can use the relevant Cloud Account Details page to switch between the two providers. Note that files uploaded with HCP provider and downloaded with HCP S3 cannot leverage the key benefits of the S3 feature.

Establishing credentials for Amazon S3

Before adding an Amazon S3 cloud account on the NAS server, you must create an Identify and Access Management (IAM) account and add an access and a secret key.

Procedure

1. Navigate to <https://console.aws.amazon.com/iam/> and log in with your user name and password. Refer to <https://console.aws.amazon.com/iam/> for more information.
2. When creating a user, generate the access and secret keys. Refer to <http://docs.aws.amazon.com/IAM/latest/UserGuide/%20ManagingCredentials.html> for more information.
3. Save the access keys to your local machine. You will need this information when you create a cloud account on the NAS server.
4. Open the page for the newly added IAM user account.
5. Attach the user policy and select **Amazon S3 Full Access** (you may have to scroll down the page).
6. Apply the policy.
7. When you create an Amazon cloud account on the NAS server, provide the new account details and access and secret keys.

Establishing a Microsoft Azure cloud account

Before adding an Microsoft Azure cloud account on the NAS server, you must create a Microsoft storage account and Primary or Secondary Access Keys.

Procedure

1. Navigate to <https://azure.microsoft.com>.
2. Log in with your user name and password.
3. Create a new storage account.
4. Obtain the Primary Access Key and Secondary Access Key for the account. See the Microsoft Azure documentation for details.
5. When you create an Microsoft Azure cloud account on the NAS server, provide the storage account details and primary access or secondary access keys.

Establishing an S3 Cloud Object Storage account

Before adding an S3 Cloud Object Storage account to the NAS server, you must create an S3 storage account and add access and secret keys. This information is required as part of the NAS server cloud account process.



Note: The procedure below is only suitable for IBM Cloud Object Storage.

Procedure

1. Navigate to <https://cloud.ibm.com/> and log in with your username and password.
2. Create a new storage account and ensure that you create access and secret keys for the user. See the S3 Cloud Object Storage help and documentation for details.
3. Create a new bucket to use as a cloud destination. See the S3 Cloud Object Storage help and documentation for details.
4. Store the user, key and bucket details for configuring the NAS server.

Importing a web server certificate

The NAS server provides some industry standard Certificate Authority certificates in its certificate store. You can upload a custom certificate if you have your own Certificate Authority or if you use self-signed server certificates.

The NAS server provides the following commands to manage custom certificates:

- **ca-certificate-show** - displays all custom certificates currently installed on the NAS server.
- **ca-certificate-import** - adds a custom X.509 certificate (contained in a PEM formatted file) to the NAS server certificate store.
- **ca-certificate-delete** - removes a custom certificate from the NAS server certificate store.
- **ca-certificate-delete-all** - removes *all* custom certificates from the NAS server certificate store.

See the command man pages for further details.

HCP certificates can be downloaded from the HCP System Management Console. See the HCP documentation for details.

Importing a certificate

Procedure

1. Save the certificate to your local machine.
2. Open a command prompt.
3. Enter the following command:


```
ssc <NAS server IP address> ca-certificate-import --path <path to certificate on local machine>
```

If the path name contains a character which has special meaning to the CLI (for example, an embedded space), put the path in quotes (").

Adding a cloud account

Procedure

1. Navigate to **Home > Storage Management > Data Migration Cloud Accounts** to display the **Cloud Accounts and Destination** page.
2. Under the Cloud Accounts section of the page, click **add** to display the **Add Cloud Account** page.

Add Cloud Account

Cloud Account Name:

Provider: Hitachi Content Platform
 Hitachi Content Platform (S3)
 Amazon S3
 Microsoft Azure
 S3 Cloud Object Storage
 Test Provider

Server Name:

User Credential:

Secret Credential:

Home | About | Sign Out

The following table describes the fields on this page:

Field/Item	Description
Cloud Account Name	The name of the cloud account.
Provider	This field identifies the cloud provider and the interpretation of remaining fields in the account definition. The options include: <ul style="list-style-type: none"> ▪ Hitachi Content Platform ▪ Hitachi Content Platform (S3) ▪ Amazon S3 ▪ Microsoft Azure ▪ S3 Cloud Object Storage ▪ Test Provider

Field/Item	Description
	Test Provider is an option that allows you to determine the outcome of the migration operation without actually moving data.
Server Name	<ul style="list-style-type: none"> ▪ For Hitachi Content Platform and Hitachi Content Platform (S3), the server name is the fully qualified domain name of the HCP namespace for the account credentials provided. The namespace for use with HCP must have an assigned owner. ▪ For Amazon S3, the server name is aws.amazon.com and is automatically inserted. ▪ For Microsoft Azure, the server name is azure.microsoft.com and is automatically inserted. ▪ For S3 Cloud Object Storage, enter the endpoint name manually (for IBM see https://ibm-public-cos.github.io/crs-docs/endpoints) ▪ For Test Provider, leave this field blank.
User Credential	<ul style="list-style-type: none"> ▪ For Hitachi Content Platform and Hitachi Content Platform (S3), this is the user name of a Data Access Account. ▪ For Amazon S3, you must have an Identify and Access Management (IAM) account. ▪ For Microsoft Azure, you must have an Azure storage account. ▪ For S3 Cloud Object Storage, you must have a Cloud Object Storage account. ▪ For Test Provider, enter <code>test</code> for the user credential.
Secret Credential	<ul style="list-style-type: none"> ▪ For Hitachi Content Platform and Hitachi Content Platform (S3), this is the password of the Data Access Account that must have the read/write/delete/purge/search permissions to the user account. ▪ For Amazon S3, this is the Secret Access Key. ▪ For Microsoft Azure, this is the primary or secondary key. ▪ For S3 Cloud Object Storage, this is the Secret Access Key. ▪ For Test Provider, enter <code>test</code> for the secret credential.

3. Enter the details of the account.
4. Click **OK** to save the account details.


Adding a cloud destination

A cloud destination associates a namespace directory for HCP and HCP (S3), a bucket for Amazon S3 or S3 Cloud Object Storage, or a container for Microsoft Azure that is tied to a cloud account.

Procedure

1. Navigate to **Home > Storage Management > Data Migration Cloud Accounts** to display the **Cloud Accounts and Destination** page.
2. Under the Cloud Destinations section of the page, click **add** to display the **Add Cloud Destination** page.

The following table describes the fields on this page:

Field/Item	Description
Cloud Destination Name	The name of the migration destination location that is tied to a cloud account. The name cannot contain spaces or any of the following special characters: " ' * / ; : < > ? \ .
Cloud Account Name	Select from the list of cloud accounts that have been added to the system.
Destination Location	Files from the primary storage are migrated to this location. For the cloud provider, this is the bucket/subfolder-list (subfolder-list is optional, but should already exist).
Encrypted In Transit	Determines if data is to be encrypted in transit. By default, HCP and HCP S3 cloud providers are not encrypted. All other cloud providers are encrypted. If the HCP destination is outside your company's firewall, be sure to encrypt in transit by manually checking the Encrypted In Transit checkbox.  Note: Data is automatically encrypted at rest when it arrives at the destination.

Viewing cloud accounts and destinations

Procedure

1. Navigate to **Home > Storage Management > Data Migration Cloud Accounts** to display the **Cloud Accounts and Destinations** page.

Storage Management [Home](#) > [Storage Management](#) > Cloud Accounts and Destinations

Cloud Accounts and Destinations

Cloud Accounts

Account Name	Provider	Server Name	User Credential
Check All Clear All			
Actions: <input type="button" value="add"/> <input type="button" value="remove"/>			
Shortcuts: Policies and Schedules Data Migration Rules Data Migration Paths			

Cloud Destinations

Destination Name	Account Name	Destination Location	Encrypted In Transit
Check All Clear All			
Actions: <input type="button" value="add"/> <input type="button" value="remove"/>			

The following tables describe the fields and columns in this page:

Item/Field for Cloud Accounts	Description
Account Name	The name of the cloud account.
Provider	Hitachi Content Platform, Hitachi Content Platform (S3), Amazon S3, Microsoft Azure, S3 Cloud Object Storage or Test Provider.
Server Name	<ul style="list-style-type: none"> ▪ For Hitachi Content Platform and Hitachi Content Platform (S3), the server name is the fully qualified domain name of the HCP namespace. ▪ For Amazon S3, the server name is aws.amazon.com. ▪ For Microsoft Azure, the server name is azure.microsoft.com ▪ For S3 Cloud Object Storage, enter the endpoint name manually (for IBM see https://ibm-public-cos.github.io/crs-docs/endpoints)
User Credential	<ul style="list-style-type: none"> ▪ For Hitachi Content Platform and Hitachi Content Platform (S3), this is the user name of a Data Access Account. ▪ For Amazon S3 this is the access key.

Item/Field for Cloud Accounts	Description
	<ul style="list-style-type: none"> ▪ For Microsoft Azure, this is the name of the storage account. ▪ For S3 Cloud Object Storage, this is the access key.
details	Displays the details of the selected cloud account settings.
add	Advances to the Add Cloud Account page where you can create a new cloud account.
remove	Deletes one or more selected data migration cloud accounts.
Policies and Schedules	Click to view existing policies and schedules. New policies and schedules can be created here as well.
Data Migration Rules	Click to view existing data migration rules. New rules can also be created here.
Data Migration Paths	Click to view existing data migration paths. New paths can also be created here.

Item/Field for Cloud Destinations	Description
Destination Name	The name of the cloud destination.
Account Name	One of the previously configured cloud accounts, selected from a list.
Destination Location	Files from the primary storage are migrated to this location. For the Amazon S3 cloud provider, this is the bucket/subfolder-list where the 'bucket' should pre-exist on the target and the 'subfolder' is optional. For the HCP and HCP S3 cloud providers, the destination location is a 'subfolder' that should pre-exist on the target. For the Azure cloud provider, this is a 'container' that should pre-exist on the target.
Encrypted In Transit	Displays Yes if Encrypted in Transmit is enabled for the cloud destination and No if it not enabled.
details	Click to view the details of the cloud destination settings.
add	Advances to the Add Cloud Destination page where you can add a new data migration cloud destination.

Item/Field for Cloud Destinations	Description
remove	Deletes the selected data migration cloud destination.

Viewing Cloud Account Details

You can view cloud account details in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Cloud Accounts and Destinations**.
2. In the Cloud Accounts section of the page, select the account to view and then click **Details** to open the **Cloud Account Details** page.

The following table describes the fields on this page:

Field/Item	Description
Cloud Account Name	The name of the cloud account.
Provider	<p>The cloud account provider.</p> <p>The supported providers are:</p> <ul style="list-style-type: none"> ▪ Hitachi Content Platform ▪ Hitachi Content Platform (S3) ▪ Amazon S3 ▪ Microsoft Azure ▪ S3 Cloud Object Storage ▪ Test Provider

Field/Item	Description
	If you are using HCP, it is possible to switch between the Hitachi Content Platform and the Hitachi Content Platform (S3) cloud providers using this page. Both providers use the same credentials and configuration options. The only difference between the two providers is the method used for file uploads and downloads. The Hitachi Content Platform (S3) cloud provider uses multi-part upload functionality. This option increases performance when using encryption or compression on HCP S series storage with Data Migrator to Cloud. See the Data Migrator Administration Guide for further information.
Server Name	<ul style="list-style-type: none"> ■ For Hitachi Content Platform and Hitachi Content Platform (S3), the server name is the URI of the name space. ■ For Amazon S3, the server name is aws.amazon.com. ■ For Microsoft Azure, the server name is azure.microsoft.com. ■ For S3 Cloud Object Storage, enter the endpoint name manually (for IBM see https://ibm-public-cos.github.io/crs-docs/endpoints)
User Credential	For Hitachi Content Platform and Hitachi Content Platform (S3), this is the user name of a Data Access Account. For Amazon S3 and S3 Cloud Object Storage, this is the access key and for Microsoft Azure, this is the primary key.
Secret Credential	The secret credential or key, shown with asterisks.

Viewing Cloud Destination Details

You can view cloud destination details in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Cloud Accounts and Destinations > Cloud Destination Details**.
2. In the Cloud Destinations section of the page, select the destination name to view and then click **Details** to open the **Cloud Destination Details** page.

The following table describes the fields on this page:

Field/Item	Description
Cloud Destination Name	The name of the cloud destination.
Cloud Account Name	One of the previously configured cloud accounts, selected from a list.
Destination Location	The location on the cloud to which files will be migrated. For the Amazon S3 cloud provider, this field is the 'bucket/subfolder' where the 'bucket' should pre-exist on the target and the 'subfolder' is optional. For the HCP, HCP S3 and Test providers, it is a 'subfolder' that should pre-exist on the target. For the Azure cloud provider it is a 'container' that should pre-exist on the target.

Viewing data migration paths

You can view the data migration paths in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Data Migration Paths**.

The screenshot shows the 'Data Migration Paths' page. At the top, there is a breadcrumb: 'Storage Management > Home > Storage Management > Data Migration Paths'. Below this is a table with the following columns: Primary File System, Primary Virtual Volume, Secondary Target Type, Secondary File System(s), EVS, and Status. There are two rows of data. The first row has 'None' for Primary File System and Primary Virtual Volume, 'Cloud' for Secondary Target Type, 'CLI-hcp-encrypt-default' for Secondary File System(s), 'mercury10-s' for EVS, and 'OK (no links exist)' for Status. The second row has 'None' for Primary File System and Primary Virtual Volume, 'WFS/HNAS' for Secondary Target Type, 'None (Test Only)' for Secondary File System(s), 'mercury10-s' for EVS, and 'OK (unused)' for Status. Below the table are links for 'Check All' and 'Clear All'. Below that is an 'Actions' section with links for 'Add WFS/HNAS Path', 'Add Cloud Path', and a 'delete' button. At the bottom, there are 'Shortcuts' for 'Policies and Schedules', 'Data Migration Rules', and 'Data Migration Cloud Accounts'.

Primary File System	Primary Virtual Volume	Secondary Target Type	Secondary File System(s)	EVS	Status	
<input type="checkbox"/> HDS	None	Cloud	CLI-hcp-encrypt-default	mercury10-s	OK (no links exist)	details
<input type="checkbox"/> HDS	None	WFS/HNAS	None (Test Only)	mercury10-s	OK (unused)	details

Check All | Clear All

Actions: [Add WFS/HNAS Path](#) [Add Cloud Path](#) [delete](#)

Shortcuts: [Policies and Schedules](#) [Data Migration Rules](#) [Data Migration Cloud Accounts](#)

The following table describes the fields on this page:

Field/Item	Description
Primary File System	The file system from which data will be migrated.
Primary Virtual Volume	If a virtual volume has been selected as primary storage, this field displays the name of the virtual volume from which data will be migrated.
Secondary Target Type	Destination target to which the data will be migrated.
Secondary File Systems	Displays the secondary file system.
EVS	The EVS hosting the file system from which data will be migrated.
Status	Status of the data migration path. The status should always be OK; if otherwise, migrated files might be inaccessible.
details	Displays the details of the selected data migration path.
Add WFS/HNAS Path	Displays the Add WFS/HNAS Path page.
Add Cloud Path	Displays the Add Cloud Path page.
delete	Deletes the specified migration policy.
Policies and Schedules	Displays the Data Migration page.
Data Migration Rules	Displays the Data Migration Rules page.
Data Migration Cloud Accounts	Displays the Cloud Accounts and Destinations page.

Adding a cloud path

You can add a cloud path in the NAS Manager.

Procedure

1. Navigate to the **Home > Storage Management > Data Migration Paths** to display the **Data Migration Path** page.
2. Click **Add Cloud Path** to display the **Add Cloud Path** page.



Note: A file system can only have one cloud target.

The following table describes the fields on this page:

Section	Item/Field	Description
Primary	EVS/File System	EVS and file system on primary storage. This defines the source for the data migration path. Click change to select another EVS or file system.
Secondary	Available	Cloud destination to which data will be migrated. Select the destination from the list. <div data-bbox="760 1052 807 1106" data-label="Image"> </div> Note: If you are creating a destination for testing purposes, you must first set up a test cloud account using Test Provider.
	Selected	Displays the selected cloud destination.

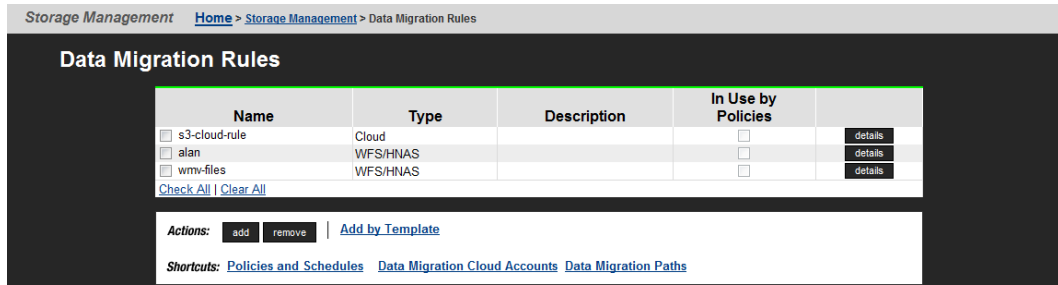
- To change the currently selected EVS and file system, click **change**.
- Select the cloud destination to which data will be migrated and move the selection to the Selected column. You can only select one cloud destination.
- Click **OK**.

Viewing data migration rules

The **Data Migration Rules** page lists all existing rules and provides for editing or removal of selected rules and creation of new rules.


Data migration rules are used in conjunction with data migration paths to form data migration policies.

Navigate to Home>Storage Management>Data Migration Rules to display the **Data Migration Rules** page.



The following table describes the fields on this page:

Item/Field	Description
Name	The name given when the rule is created. It is used to identify the rule when creating or configuring policies.
Type	The type of data migration that this rule can be used for.
Description	A description of the rule to help identify the criteria to be applied.
In Use by Policies	The check box is filled when a rule is being used by one or more policies.
details	Click for a selected migration rule to display its complete details.
add	Click to create custom rules that will define the criteria by which the files will be migrated.
remove	Click to remove one or more existing rules.
Add by Template	Click to create simple rules using predefined templates.
Policies and Schedules	Goes to the Data Migration Policies and Schedules page. New policies and schedules can be created there.
Data Migration Cloud Accounts	Goes to the Cloud Accounts and Destinations page. New cloud accounts and destinations can be created there.
Data Migration Paths	Goes to the Data Migration Paths page. New paths can be created there.

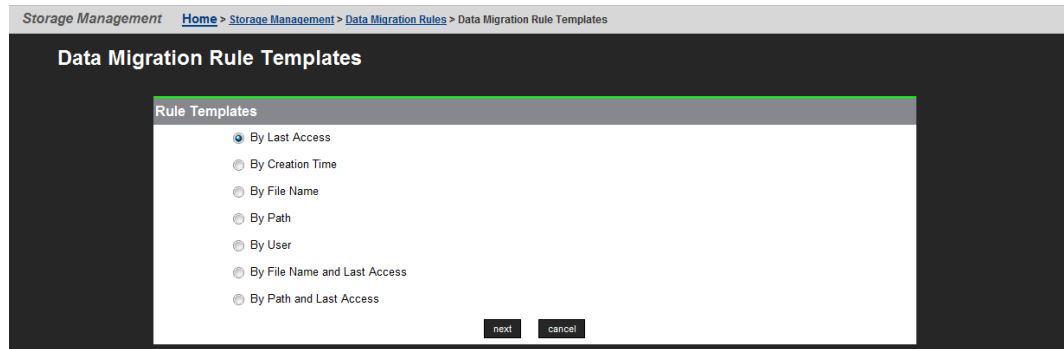
 **Caution:** Once created, do not change a data migration rule without verifying that it is not used by existing policies, as such changes might result in unintentional changes to existing policies.

Adding a data migration rule by template

Rules define the properties of files that will be migrated.


Procedure

1. To create rules that suit more specific migration needs, navigate to **Home > Storage Management > Data Migration Rules** to display the **Data Migration Rules** page, and then click **Add by Template** to display the **Data Migration Rule Templates** page:



2. Select a **Rule Template**, then click **next**.
The following table describes each of the available rule templates:

Rule Template	Description
By Last Access	Migrates all files that have remained inactive (or have been active) within a certain period of time.
By Creation Time	Migrates all files created before or after a specific point in time.
By File Name	Migrates all files with the same name and extension. An asterisk can be used as a wildcard character. For example: <ul style="list-style-type: none"> ▪ <code>dbfile.db</code> migrates all files with the name <code>dbfile</code> and the extension <code>.db</code>. ▪ <code>*.db</code> migrates any file with an extension of <code>.db</code> regardless of the file name. ▪ <code>dbfile.*</code> migrates all files with the name <code>dbfile</code> and any extension.

Rule Template	Description
	<ul style="list-style-type: none"> *dbfile.db migrates all files ending with the name dbfile and the extension .db. dbfile* migrates all files with a name beginning with dbfile and having any extension.
By Path	Migrates all files under a particular directory.
By User	Migrates all files of the specified users. <div style="border: 1px solid black; background-color: #e0f2f1; padding: 5px; margin-top: 10px;">  Note: This rule does not apply to the Data Migrator to Cloud. </div>
By File Name and Last Access	Migrates files of a certain name and/or extension (as described above) that have remained inactive for a certain period of time.
By Path and Last Access	Migrates all files under a certain directory that have remained inactive for a certain period of time.

3. Enter requested template-specific information:

- If you select **By Last Access**, the **Data Migration Rule: Last Access Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Include Criteria	To specify the maximum period a file can be inactive before being migrated to a secondary file system: <ol style="list-style-type: none"> From the menu, select inactive. The menu includes an option for selecting the opposite scenario; that is, to choose active within to specify files that have been active within the specified period. From the menu, select the period (days, hours, or minutes). Enter the threshold quantity period.

- If you select **By Creation Time**, the **Data Migration Rule: Creation Time Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Include Criteria	To specify the point in time for the migration rule: <ol style="list-style-type: none"> From the first menu, select more than or less than. Enter the threshold number. From the second menu, select month(s), week(s), day(s), hour(s), or minute(s).

- If you select **By File Name**, the **Data Migration Rule: File Name Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Include Criteria	To specify the type of files (based on their file extension) to be migrated to a secondary file system: <ol style="list-style-type: none"> From the menu, select include. The menu also has an option for selecting the opposite scenario; that is, selecting to exclude files not of the specified type. In the all files named field, enter the file name and extension. More than one file name or extension can be named in this field separated by commas; for instance: *.jpg, *.bmp, *.zip.

- If you select **By Path**, the **Data Migration Rule: Path Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Include Criteria	To specify the path to the files under a certain directory: <ol style="list-style-type: none"> From the menu, select include. The menu also has an option for selecting the opposite scenario; that is, to select exclude to select all files that are not in the path. In the all files in the path field, enter the directory file path.

- If you select **By User**, the **Data Migration Rule: User Name Template** page contains the fields described in the following table:



Note: This option only applies to WFS/HNAS and does not apply to Data Migrator to Cloud.

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	You can only enable the WFS/HNAS option. This rule does not apply to cloud options.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Include Criteria	To specify the user names for the owners of the files to be migrated to a secondary file system: <ol style="list-style-type: none"> From the menu, select include. The menu also has an option for selecting the opposite scenario; that is, selecting to exclude files from owners other than the specified owners.

Item/Field	Description
	<p>b. In the all files in the path field, enter the UNIX or Windows user names for the owners of the files you want to migrate. More than one user name can be listed in this field, but names must be separated by commas. For instance, <code>jjames, myco\smithr, myco\smith</code>.</p> <p>Windows user names are specified in the form <code>domain\user name</code>, and backslashes in user names should not be escaped (double backslashes are not required).</p>

- If you select **By File Name and Last Access**, the **Data Migration Rule : Last Access Time and File Name Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, fill this check box.
Include Criteria	<p>To migrate inactive files from a specified directory to a secondary file system:</p> <ul style="list-style-type: none"> a. In the All files named field, enter the file name extension of the files to be migrated. For example <code>note.txt</code>, <code>note*</code>, or <code>mp3</code>. b. In the All files not accessed within___ field, enter the threshold quantity. c. Select the period from the list. You can choose days, hours, or minutes.

- If you select **By Path and Last Access**, the **Data Migration Rule: Last Access Time and Path Template** page contains the fields described in the following table:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	The type of data migration that this rule can be used for.
Case-sensitive pattern checks	To specify case-sensitive rule checking, fill this check box.
Include Criteria	To migrate inactive files from a specified directory to a secondary file system: <ol style="list-style-type: none"> a. In the All files in the Path field, enter the directory file path. b. In the All files not accessed within___ field, enter the threshold quantity. c. Select the period from the list. You can choose days, hours, or minutes.

4. Verify your settings, then click **OK** to save or **cancel** to decline.

Adding a data migration rule for the Data Migrator to Cloud

This page can be used to name, define, add, and modify Data Migration Rules using rule syntax. Rules can be built with a series of INCLUDE and EXCLUDE statements. Each of these statements can contain a number of expressions specifying the type of files and the conditions under which they will be migrated.

For example:

```
INCLUDE (<FILENAME *.mp3> AND <FILE_SIZE_OVER 2GB>)
```

Procedure

1. Navigate to **Home > Storage Management > Data Migration Rules** to display the **Data Migration Rules** page and then click **add**.

The following table describes the fields on this page:

Item/Field	Description
Name	Enter a name for the new rule. The rule name can include only alphanumeric characters, hyphens, and underscores.
Description	Enter a description of what the rule does.
Type	Click the appropriate option, either WFS/HNAS or Cloud.
Case-sensitive pattern checks	To specify case-sensitive rule checking, select this check box.
Rule Definition	Insert the syntax for the data migration rule.



Note: For Data Migrator to Cloud only, files that are 4,096 bytes or less will not be migrated.

2. Verify your settings, then click **OK** to save the rule, or click **cancel** to decline.
For Data Migrator to Cloud only, note that files that are 4,096 bytes or less will not be migrated.

Modifying a data migration rule

You can modify a data migration rule in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Data Migration Rules**.
2. Select the check box next to the rule to modify and then click **details**.

The following table describes the fields on this page:

Field/Item	Description
Name	Displays the name of the rule.
Description	The description of the rule. Make any changes as appropriate.
In Use by Policies	Displays any associated policies in use for this policy. If none are used, displays 'Not in use.'
Type	Displays the type of rule, either Cloud or WFS/HNAS.
Case-sensitive pattern checks	Select the check box if the rule checking must be case sensitive.
Rule Definition	Displays the current definition in use. Modify if necessary.

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

Viewing data migration policies and schedules

Having created both data migration paths and data migration rules, data migration policies can now be created. Policies assign a rule or set of rules to a specific data migration path. They also define the conditions that initiate data migrations.

Procedure

1. To view data migration policies, navigate to **Home > Storage Management > Data Migration** to display a list of policies and schedules.

The screenshot displays the 'Data Migration' management page. At the top, there is a breadcrumb trail: 'Storage Management > Home > Storage Management > Data Migration'. The main content is divided into two sections: 'Policies' and 'Schedules'.

Policies Section:

Name	EVS	Primary File System	Secondary File System	Rule	
<input type="checkbox"/> CloudMigration1	mercury10-s	HDS	CLI-hcp-encrypt-default	s3-cloud-rule	details


Below the table are links for 'Check All' and 'Clear All'. An 'Actions' box contains 'add' and 'remove' buttons. A 'Shortcuts' section lists: [Data Migration Rules](#), [Data Migration Cloud Accounts](#), [Data Migration Paths](#), and [NDMP Configuration](#).

Schedules Section:

Policy Name / Schedule ID	EVS	Next Run	Migration Type	Last Status	
<input type="checkbox"/> CloudMigration1 / 5	mercury10-s	2014-05-30 00:00:00 (UTC-0700)	Migrate files (daily)	No Status	details

Below the table are links for 'Check All' and 'Clear All'. An 'Actions' box contains 'add', 'remove', 'run now', and 'Stop Migration(s)' buttons. A 'Shortcuts' section lists: [Data Migration Status & Reports](#).

The following tables describe the fields on this page:

Item/Field for Policies	Description
Name	Name of a data migration policy.
EVS	Primary EVS from which the migration originates.
Primary File System	Files in the primary file system or virtual volume that will be migrated.
Secondary File System	Secondary file system, to which all data will be migrated to.  Note: If the path to the secondary file system is an external path, the name or IP address of the server hosting the secondary file system is also displayed in parentheses. The displayed server name/IP address is a link, and you can click the link to display the full path.
Rule	Rules that can be triggered in this migration policy.
details	Displays the details for the selected policy.
add	Advances to the Add Data Migration Policy page.
remove	Deletes the selected migration policy.
Data Migration Rules	Advances to a page where all the configured data migration rules will be displayed. New rules can be created here as well.
Data Migration Cloud Accounts	Advances to the Cloud Accounts and Destinations page.
Data Migration Paths	Displays the configured data migration paths. New paths can be created as well.
NDMP Configuration	Advances to a page where the NDMP can be configured by entering the username, password, and NDMP version number.

Item/Field for Schedules	Description
Policy Name/Schedule ID	Displays the name given to the Data Migration Policy
EVS	Displays the primary EVS from where the migration is scheduled to originate.
Next Run	Displays the month, date, year and time for the next scheduled data migration run for this policy.

Item/Field for Schedules	Description
Migration Type	Displays the type of data migration that has been scheduled to run: <ul style="list-style-type: none"> ▪ Migrate files (followed by only once, daily, or weekly depending on the selected scheduled type). ▪ Simulate migration - Generates a one-time report of files that would be migrated. Does not actually migrate files. ▪ Report migrated files - Generates a one-time report with a list of previously migrated files. This migration type only applies to WFS/HNAS and not Data Migrator to Cloud.
Last Status	Displays the final status of the last run of the data migration operation.
details	Displays the current settings for the selected schedule.
add	Advances to the Add Data Migration Schedule page.
remove	Deletes the selected migration policy.
run now	Starts the scheduled data migration immediately.
Stop Migration(s)	Click the Stop Migrations link to stop a selected, in-process migration. Only migrations in progress can be stopped.
Data Migration Status & Reports	Advances to a page where all the completed migration runs will be listed in detail.

Adding a cloud data migration policy

You can add a cloud data migration policy in the NAS Manager.

Procedure

1. Navigate to **Storage Management > Data Migration** and then click **add** under the Policies section to display the **Add Data Migration Policy** page.

Storage Management [Home](#) > [Storage Management](#) > [Data Migration](#) > Add Data Migration Policy

Add Data Migration Policy

Policy Identification

Name:

Migration Path

Migrate Data

Primary EVS / File System: donotdelete / donotdelete
Virtual Volume: -

Secondary Target Type: Cloud
Secondary File System: DM3

Reverse Migrate

EVS / File System: donotdelete / donotdelete

Reverse migration is not available for cloud destinations.

(To create paths, see [Data Migration Paths](#))

Pre-conditions

Available Cloud Rules

PNGs
Files

when primary file system free space is less than %

when other conditions are not met

Selected Cloud Rules

(To create rules, see [Data Migration Rules](#))

The following table describes the fields on this page:

Item	Description
Policy Identification	This section allows you to specify a name to identify the migration policy.
Name	Name for the new data migration policy.
Migration Path	This section allows you to specify the data migration path to be used by the migration (or reverse migration) policy.
Migrate Data	When creating a migration policy, this section displays the data migration source and target information: <ul style="list-style-type: none"> ▪ Primary EVS/File System: Displays the name of the EVS and file system for primary storage (the migration source). ▪ Virtual Volume: Virtual volumes do not apply to the Data Migrator to Cloud.

Item	Description
	<ul style="list-style-type: none"> ▪ Secondary Target Type: Displays Cloud to represent the migration type. ▪ Secondary File System: Displays the name of the file system on secondary storage that will host the migrated data (the migration target).
Reverse Migrate	This option does not apply for cloud destinations.
change...	Click this button to open the Select a Path page to select a different path.
(To create paths, see Data Migration Paths)	Advances to the Data Migration Paths page, which allows you to create data migration paths.
Pre-Conditions	This section allows you to specify the rules (the criteria) that the files must match/meet in order to be migrated or reverse migrated (reverse migration is for Data Migrator only not Data Migrator to Cloud) by this policy.
Available Cloud Rules	<p>Rules with specific threshold limits are displayed here. This list of rules define the set of conditions which trigger the migration/reverse migration. You can:</p> <ul style="list-style-type: none"> ▪ Add a Pre-condition to the Selected Rules list by selecting it and clicking the right arrow (>). ▪ Remove a rule from the Selected Rules list by selecting it and clicking the left arrow (<). <p>This policy will be run either according to a defined schedule, or when started manually. Once the policy is run, the threshold specifies when the selected rules are applied. You can specify that the selected rules will be applied when either of the following conditions are met:</p> <ul style="list-style-type: none"> ▪ When the primary file system's free space falls below X% (set the percentage level for this condition). ▪ When other conditions are not met. These conditions are defined in the selected rule(s). <p>After selecting rules and the threshold, save the policy by clicking OK.</p>
Selected Cloud Rules	Displays the rules containing the criteria/conditions to be used to determine if a file should be migrated. The criteria in the rules are applied when the threshold (the when condition specified in the Available Rules section) is met.

Item	Description
(To create rules, see Data Migration Rules)	Advances to the Data Migration Rules page, which allows you to create rules.

Using Pre-Conditions

When a migration policy is scheduled to run, it evaluates the percentage of available free space in the Policy's primary storage. Based on this analysis, one rule may be triggered to define the data set subject to migration. Migrations of data from primary storage then occurs based on the statements in the rule that was triggered. Only a single rule will be engaged during any particular migration operation.

When defining pre-conditions, customer support recommends aggressive tiering; specifically, it may be desirable to migrate .mp3 files and the contents of the directory /tmp regardless of the available free space. Then, if free space on primary storage is reduced to less than 50%, also to migrate all files not accessed within the last sixty days. Finally, if available free space is reduced to less than 15%, also to migrate the contents of users' home directories.

The following rules illustrate this scenario:

Rule	Statement
Rule 1:	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>
Rule 2:	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>
	INCLUDE (<INACTIVE_OVER 60>)
Rule 3:	INCLUDE (<FILENAME *.mp3>) OR <PATH /tmp/*>
	INCLUDE (<INACTIVE_OVER 60>)
	INCLUDE (<PATH /home/*>)

Related pre-conditions

- Rule 3 if free space is less than 15%.
- Rule 2 if free space is less than 50%.
- Rule 1 if no other condition applies.

When the migration policy is scheduled to run, different rules may be triggered based on the available free space on primary storage. When a migration policy is engaged, only a single rule will be triggered to run.

For example:

- If free space is at 80%, then Rule 1 will be used.
- If free space is at 40%, then Rule 2 will be used.
- If free space is at 10%, then Rule 3 will be used.

When percentage thresholds are specified, they are evaluated based on whole number percentages. This means that if two rules are specified, one that will take effect at 8% of free space and one at 9% of free space, if the file system has 8.5% free space available, then the rule with the 8% pre-condition will apply.



Note: If the primary storage defined in the migration path is a virtual volume, free space will be based on the limit defined by the virtual volume quota. If a virtual volume quota has not been defined, then free space available will be based on the free space of the file system hosting the virtual volume.

Connection Errors

When attempting to add a new migration policy, a connection error may be indicated by a message saying "Unable to connect to <IP address>" or "Error accessing <source/destination> server".

The "Unable to connect to" message means one of the following:

- The server is not currently powered up or is temporarily disconnected from the network. The server must be available and properly connected when creating a migration policy.
- The Gigabit Ethernet port providing access to the EVS which hosts the File System is not accessible from the SMU. This may be the case if the network is set up with private subnetworks as commonly used with VLANs. In this case, the server may have been configured so that SMU access is through the management ports instead of the ports set using the `ndmp-management-ports-set` command.

The "Error accessing server" message may occur as a result of restricting NDMP access using the `ndmp-option` command. The `allowip` and `blockip` options can be set such that the SMU is not allowed to access the NDMP services via the standard routes. If the NDMP connection restrictions are definitely required, change the configuration of the server to allow SMU access via the management ports using the `ndmp-management-ports-set` command. The SMU connections then bypass the `allowip/blockip` checks.

Modifying a data migration policy

You can modify a data migration policy in the NAS Manager.

Procedure

1. Navigate to **Home > Storage Management > Data Migration**.
2. Select the policy to modify and then click **details** to display the **Modify Data Migration Policy** page.

The following table describes the fields:

Item	Description
Policy Identification	Name of the data migration policy.
Migration Path	The specified data migration path to be used by the migration (or reverse migration) policy.
Pre-Conditions	This section allows you to modify the rules (the criteria) that the files must match/meet in order to be migrated (or reverse migrated) according to this policy.
Available Rules	<p>Rules with specific threshold limits are displayed here. This list of rules define the set of conditions which trigger the migration/reverse migration. You can:</p> <ul style="list-style-type: none"> ▪ Add a Pre-condition to the Selected Rules list by selecting it and clicking the right arrow (>). ▪ Remove a rule from the Selected Rules list by selecting it and clicking the left arrow (<). <p>This policy will be run either according to a defined schedule, or when started manually. Once the policy is run, the threshold specifies when the selected rules are applied. You can specify that the selected rules will be applied when either of the following conditions are met:</p> <ul style="list-style-type: none"> ▪ When the primary file systems free space falls below X% (set the percentage level for the condition). ▪ When other conditions are not met. These conditions are defined in the selected rule(s). <p>After selecting rules and the threshold, save the policy by clicking OK.</p>
Selected Rules	Displays the rules containing the criteria/conditions to be used to determine if a file should be migrated. The criteria in the rules are applied when the threshold (when condition specified in the Available Rules section) is met.
(To create rules, see Data Migration Rules)	Advances to the Data Migration Rules page, which allows you to create rules.

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

Migration schedules

After a data migration policy has been defined, it must be scheduled. The decision on how often to run a policy may be affected by the rules selected in this policy. For example:

- A policy with a single rule to migrate all `.mp3` files may be scheduled to run once every month.
- Another policy, used to archive a working `/project` directory once the project is complete, may be scheduled as a Once Only Schedule.
- Other policies which migrate based on various Pre-conditions, and are triggered on available free space, may be scheduled to run every week.

When planning migration schedules, schedule migrations during off-peak times, such as evenings and weekends.

After a data migration has begun, additional data migrations for the same policy cannot be started until the current one has completed. However, it is possible to start multiple concurrent data migrations if each have its own policy.

Adding a Data Migration schedule

You can add a data migration schedule in the NAS Manager.



Note: You must create a migration policy before you can schedule a migration.

Procedure

1. Navigate to **Home > Storage Management > Data Migration**.
2. Click **add** in the Schedule section of the page to display the **Add Data Migration Schedule** page:

The screenshot shows the 'Add Data Migration Schedule' page. The breadcrumb navigation is 'Storage Management > Home > Storage Management > Data Migration > Add Data Migration Schedule'. The form contains the following fields:

- Data Migration Policy:** CloudMigration1 (Cloud)
- Migration Type:** Migrate Files (daily)
- Simulate Migration:** generate a report of files that would be migrated. Does not actually migrate files. Only run once.
- Report Migrated Files:** generate a report with a list of previously migrated files. Only run once.
- Date and Time to Start:** Start data migration on 2014-05-30 at 00:00 (24 hour time). (Current date and time on mercury10: 2014-05-29 12:09:34 (UTC-0700))
- Duration Type:** Run until migration completes.
- Suspend migration after:** 2:00 Hours:Minutes. Resume when the next schedule starts.

Buttons for 'OK' and 'cancel' are visible at the bottom of the form.

The following table describes the fields on this page:

Field/Item	Description
Data Migration Policy	Select a migration policy from the list.
Migration Type	<p>Choose from the following migration type options:</p> <p>Migrate Files: Select this option and then choose only once, daily, or weekly, from the list. Selecting the Once Only option causes the policy to run only once, at the specified date and time.</p> <p>Simulate Migration: Select this option to generate a report of files that would be migrated. Does not actually migrate files. Only run once.</p> <p>Report Migrated Files: Select this option to generate a report with a list of previously migrated files. Only run once. This option only applies to WFS/HNAS and does not apply to Data Migrator to Cloud.</p>
Date and Time to Start	<p>Specifies when the policy will run.</p> <p>From the calendar next to the field, select the start date for the policy's initial run. The selected date appears on the field.</p> <p>Enter the scheduled run time in a 24 hour setting (for example, 11:59 PM will be entered as 23:59). The current NAS Manager date and time are provided below for reference.</p>
Duration Type	<p>Choose from the following duration types:</p> <p>Run until migration completes indicates that the scheduled policy should run until it has completed.</p> <p>Suspend migration after x Hours:Minutes. Resume when the next schedule starts indicates the scheduled policy should be suspended after the time specified and resumed at the next scheduled interval. Note that this option only applies to Data Migrator to Cloud and not to WFS/HNAS.</p>

3. Verify your settings. Then click **OK** to save or **cancel** to decline.

Modifying a schedule

Once defined, schedules can be easily modified to meet the changing requirements of data migration policies. When modifying a schedule, the scheduled date and time, as well as the interval in which the schedule will run can be changed.

Procedure

1. Navigate to **Home > Storage Management > Data Migration**.
2. Under the Schedules section of the page, fill the check box next to the schedule to modify and then click **details**.

The following table describes the fields on this page:

Field/Item	Description
Data Modify Policy	Name of the schedule. This is a read-only field.
Data Migration Type	The type of migration: WFS/HNAS, External, or Cloud.
Migration Type	<p>Displays the current option.</p> <p>Migrate files - options are:</p> <ul style="list-style-type: none"> ▪ only once ▪ daily ▪ weekly <p>Simulate Migration - Generates a report of files that would be migrated. Does not actually migrate files. Only run once.</p> <p>Report Migrated Files - Generates a report with a list of previously migrated files. Only run once. This option applies to WFS/HNAS and External data migration types and does not apply to Data Migrator to Cloud type.</p>
Next Run	Date and time of next scheduled run.
Initial Run	Date and time of initial run.
Reschedule	To change this, fill in the check box and enter the new date and time.
Duration Type	<ul style="list-style-type: none"> ▪ Run until job completes indicates that the scheduled policy should run until it has completed ▪ Suspend migration after x Hours:Minutes. Resume when the next schedule starts indicates the scheduled policy should be suspended after the time specified and resume at the next scheduled interval. Note that this option only applies to the Data Migrator to Cloud.

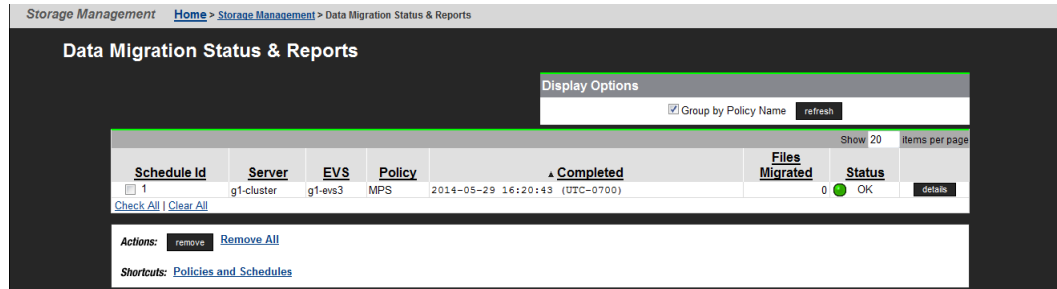
3. Make any modifications as necessary.
4. Click **OK**.

Data Migration status and reports

After a data migration policy has completed a cycle, it generates a data migration report that includes details about files migrated, including available free space before and after the migration. Reports of the last five scheduled migrations are routinely saved; the rest are purged. If a schedule is deleted, so are its reports.

Migration reports can be downloaded in CSV format, then imported into a spreadsheet and processed, saved, or printed. These reports are useful when studying the system access patterns, file storage tendencies, the efficiency of rules, paths, policies and schedules. By gauging file and space usage statistics of Primary and secondary storage, Data Migrator reports can be used to refine a rule or pre-condition. The more precise and aggressive the rule, the better Data Migrator serves the storage system.

To view a list of existing reports, navigate to Home>Storage Management>Data Migration Status & Reports.



The following table describes the fields on this page:

Item	Description
Display options: Group by policy name	Selecting this option groups the data migrations by policy name, even if they are sorted in a different order, for example, the completed time and date.
Schedule ID	ID number for the completed migration.
Server	Primary file system's server.
EVS	Primary file system's EVS.
Policy	Policy name.
Completed	Year, month, day and time when the migration was completed.
Files Migrated	Number of files that were migrated.
Status	Migration completion status.
details	Opens the Data Migration Report page where you can view the details of the select report.
remove	Click to remove a selected report.
Remove All	Click to remove all migration reports in the list.
Policies and Schedules	Opens the Policies and Schedules page where you can view, add, and remove existing policies and schedules.

Viewing details of a data migration cloud report

To view data migration reports, navigate to Home>Storage Management>Data Migration Status & Reports, and then click details to display the **Data Migration Report** page:

Storage Management [Home](#) > [Storage Management](#) > [Data Migration Status & Reports](#) > Data Migration Report

Data Migration Report

Report Summary

Migration Policy: MPS
 Schedule ID: 1
 Status: ● OK [View Log](#)
 Migration Type: Migrate files
 Frequency: Daily

Start Time: 2014-05-29 16:20:43 (UTC-0700)
 End Time: 2014-05-29 16:20:43 (UTC-0700)
 Duration: 00:00:00

Server / EVS: g1-cluster / g1-eva3
 Rule Used: None
 Amount Migrated: 0 Bytes
 Files Migrated: 0
 Files Failed: 0

PHDS1 - Primary File System Statistics						File System Capacity	Live File System Reclaimed	Total File System Reclaimed
Pre-Migration File System Space Used			Post-Migration File System Space Used					
Live FS	Snapshots	Total Usage	Live FS	Snapshots	Total Usage	500.75 GB	0 Bytes (0 %)	0 Bytes (0 %)
3.90 GB (1%)	0 Bytes (0%)	3.90 GB (1%)	3.90 GB (1%)	0 Bytes (0%)	3.90 GB (1%)			

Actions: [back](#) [delete](#) | [View Log](#) [Download Migration Report](#)

The following table describes the fields on this page:

Item	Description
Report Summary	
Migration Policy	Completed migration policy name.
Schedule ID	Migration schedule ID.
Status	Migration completion status.
Migration Type	Type of migration, migrate files, simulate migration, report migrated files.
Frequency	How often the Policy is scheduled to run.
Start Time	Date and time when the migration began.
End Time	Date and time when the migration ended.
Duration	Duration of migration.
Server/EVS	EVS on which the Primary and secondary storage reside.
Rule Used	Rule used by the policy.
Amount Migrated	The migrated amount of data, in GB.
Files Migrated	Quantity of files that were migrated. If files have been migrated, click this to view a list of the files that were migrated. The list provides details on their path, size, and their start and end times.
Files Excluded	Number of files that should have been migrated but were not. For example, files in use at the time of the migration may not be migrated.
Primary File System Statistics	
Pre-Migration File System Space Used	File system size, snapshot size, and the total used space before the migration.
Post-Migration File System Space Used	File system size, snapshot size, and the total used space after the migration.
File System Capacity	File system's total capacity.
Live File System Reclaimed	Reclaimed space in the live file system, defined as the usable space on the file system; that is, the part of the file system not reserved or in use by snapshots.
Total File System Reclaimed	Reclaimed space in the total file system, defined as the entire capacity of the file system and includes usable space and space that is reserved or in use by snapshots.

The following Actions are available:

- Click View Log to view a log file containing time, duration and status details of the migration. A View Log link is available at both the top and bottom of the page.
- Click Download Migration Report to view a report about the completed data migrations with details on the primary and secondary file systems and virtual volumes, including status, space utilization before and after the migration, the duration, start, and end time for the migrations.

Included in the download are two other important reports: one that lists all the files that were migrated (list.gz) and the other that lists all the files that were not migrated (failed.gz).

Cloud data migration and replication considerations

The following lists important data migration and replication considerations.

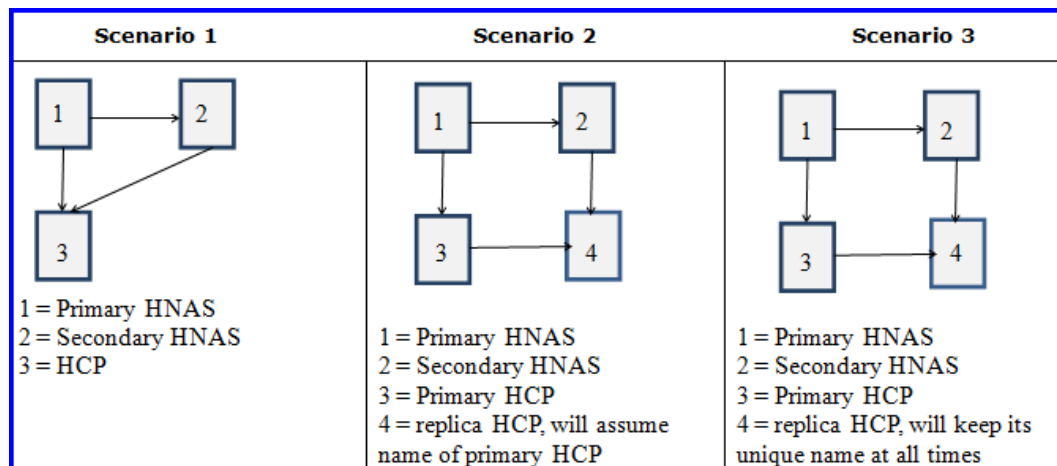
Amazon and file-based replication

You may decide to deploy a replicated environment to protect primary and archived data against site-wide failures. When using file replication in conjunction with HCP replication, special configuration is required. The special configuration depends on the HNAS and HCP replication scenario.





Note: In order to take advantage of the new enhancements to HCP as a target, you need to recall all the data and then re-setup your schedules and policies, using the new Data Migrator to Cloud.

Consider the following three scenarios when using Data Migrator to Cloud to HCP along with file replication and HCP replication:



Caution: Care should be taken when configuring systems with a single migration destination for both replication source and target (known as a triangular arrangement). Such arrangements should not be considered a valid solution in any disaster recovery (DR) or backup scenario, as there is only a single copy of the user data pointed to by XVLs at each end of the replication policy.

Scenario 1	<p>Illustrates replicating file systems between clusters, both of which point to a single HCP system, presumably hosted elsewhere; however, it is possible that the primary system and HCP system are in the same location.</p> <div style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"> <p> Caution: In this scenario, both clusters/entities map to the same HCP system. With file replication it is possible to access the secondary file system(s) at any time. It is strongly recommended to keep the destination file system syslocked to avoid unintentional deletion of data on the HCP system.</p> </div>
Scenario 2	<p>Illustrates replicating file systems between clusters, where each cluster points to a local HCP system. The HCP systems replicate migrated data and also perform a DNS failover so that the secondary HCP maintains the same name resolution as the primary system.</p> <div style="background-color: #e0f7fa; padding: 10px; border: 1px solid #ccc;"> <p> Note: In this scenario, HCP uses a DNS failover capability. Due to the way the HCP failover functionality operations, the secondary will also point to the primary HCP. With file replication it is possible to access the secondary file system(s) at any time. It is strongly recommended to keep the destination file system syslocked to avoid unintentional deletion of data on the HCP system.</p> </div>
Scenario 3	<p>Illustrates replicating file systems between clusters, where each cluster points to a local HCP system. The HCP systems replicate migrated data and maintain their own unique name resolution.</p>

Scenario 3

For scenario 3, the cloud account must be configured as follows:

1. Create a "dummy" namespace on the secondary HCP system with the same namespace and tenant name as the primary system. The HCP system and the domain will then be different.
2. Create a namespace data access user with read-write permissions on the "dummy" namespace.
3. Configure a cloud account to this namespace, which will confirm the read-write permissions.
4. Remove the namespace and then configure replication in HCP to create a replica namespace on the secondary system. Because a replica is read-only until a failover, the read-write permissions check performed by the cloud account creation command will fail unless this "dummy" is created.

Scenario 1 and 2

For scenarios 1 and 2 the cloud account creation command must specify the namespace and data access account of the primary HCP system.

All Scenarios

For all scenarios, the cloud destination must be configured as follows:

1. The destination path and UUID must be the same at the secondary and the primary because the stub contents will be replicated between clusters and the stub contains the path UUID of the destination. If the path and UUID changes between clusters, Data Migrator to Cloud cannot locate migrated files after a failover.
2. Identify the UUID of the cloud destination object in the primary file system. This can be performed using the BOS CLI with the following command:
 - `migration-cloud-destination-list <destination-name>`
 - "Destination ID" is the UUID of this destination
 - "Path at destination" is the path
3. On the secondary file system, configure the cloud destination object using the BOS CLI (not the SMU), specifying the UUID with the `-u` option, For example:
 - `migration-cloud-destination-create <destination_name> -a <account_name> -p <path at destination> -t yes -u <UUID (obtained above)>`
 - The `-p` option should specify the path that was created at the primary.
 - The `-u` option is the UUID of the destination at the primary

Cloud Objects

All other cloud objects (Data Migration paths, rules, policies, and schedules) are configured the same as in a non-replicated environment.

- Data migration paths are not copied by file-based replication. As with Data Migrator, the XVLs will work correctly only if the cloud path exists on the replication target. The path must be created prior to the start of replication.
- Data Migrator policies and schedules are not copied with file-based replication. You must manually re-create them on the replication target to support continuing migration to the cloud.
- For the cloud, you must create the replication rule (navigate to Home > Data Protection > File Replication Rules), using the values below instead of the default settings. This ensures that replication copies the migration links and allows access to the migrated data. Make sure the replication rule is correctly specified in the replication policy.
 - Migrated File Remigration = Enabled
 - External Migration Links = Re-create link

See the Replication and Disaster Recovery Administration Guide for more information.

Finally, to preserve bandwidth when replicating data between HNAS systems, instruct file replication to only migrate the stubs and not the actual data, which will be replicated by HCP itself. To do this, perform the following steps:

- When creating a file system replication rule, set the "External Migration Links" setting to "re-create links." On the BOS CLI, run the following commands:
 - `evssel <evs number of the file system>`
 - `migration-recreate-links-mode always-recreate-links`

Multi-site HCP and file-based replication

- The same considerations as described in the Amazon and file-based replication apply to multi-site HCP and file-based replication.
- The replication of the migrated data HCP -> HCP must be performed by HCP. It is recommended that the server name and credentials be the same for both the source and the target. If this is not possible, it can be done at the cloud account and destination level.

The path as replicated will point to the original cloud destination, and can be redefined if a different destination is desired. Data migration to the cloud will not begin until after disaster recovery occurs.



Caution: If both the source and destination point to the same HCP, the destination file system should be syslocked to prevent unintentional deletion of data.

Object-based replication

When using object replication, the default behaviour is to 'rehydrate' data that has been migrated using either external migration or the Data Migrator to Cloud (DM2C) feature. Files that have been converted to External Volume Links (XVLs) are copied in full to the replication target.

The NAS server is also able to copy XVLs as links without having to re-inflate them at the destination target. The configuration of this functionality is discussed in detail in the Replication and Disaster Recovery Admin guide section "Transferring XVLs as links during object replication".

NDMP backup

Hitachi NAS NDMP offers several variables to control how migrated (tiered) data is handled during backup and restore. These variables can typically be controlled through the backup application, and the way in which they are called is specific to each backup platform. For example, In NetBackup, environment variables can be set within the backup selections list by specifying one or more SET directives in a stanza. Consult the documentation of the Backup application for specific guidance.

There are two main NDMP variables that control behavior of migrated files:

- `NDMP_BLUEARC_EXCLUDE_MIGRATED`: Controls how an NDMP backup interacts with CVL (files that have been migrated internally, for example, from SAS to NL-SAS). The Valid values are y or n. If set to y , the backup or copy will not include files whose data has been migrated to another volume. The default setting is n meaning that migrated files and their data will be backed up as normal files. The backup/copy retains the information that these files had originally been migrated.
- `NDMP_BLUEARC_EXTERNAL_LINKS`: Controls how an NDMP Backup interacts with XVLs (files that have been migrated to an external storage tier / cloud provider). The valid value are `remigrate`, `ignore` and `recreate_link`.
 - If set to `remigrate`, externally migrated files and their data will be backed up as normal files. On recovery the file will be restored and then an attempt will be made to remigrate the file to external storage again.
 - If set to `ignore`, the backup or copy will not include files whose data has been migrated externally.
 - If set to `recreate_link` , the backup or copy will include details of the link but none of the data contents. On recovery an attempt will be made to recreate the link to an existing file on the external storage system.

For platforms such as TSM that cannot directly manipulate NDMP variables, the CLI `ndmp-option` command `backup_ignore_external_links` option exists to allow the backup platform to ignore files migrate to external storage tiers.

For further details please consult the NDMP Backup Administrator Guide.



Note: If the `xvl-auto-recall-on-read` environment variable is enabled, an NDMP job will not cause the migrated files to be recalled.

Virtual Server Security

The Virtual Secure Servers feature is compatible with Data Migrator to Cloud, provided the following requirements are met:

- A cloud target can be resolved in a DNS server configured in Global Context.
- A route from the aggregate ports to the cloud provider server (HCP, HCP S3, AmazonS3, S3 Cloud Object Storage or Azure) exists on all nodes.

Multi-tenancy

Multi-tenancy is not supported with Data Migrator to Cloud.

Other configurations

Other configurations may be possible. If your environment differs from the scenarios described above, contact customer support or your Global Solutions and Services representative.

Introduction to HCP no delete feature

The HCP "no delete" feature adds an extra level of data protection by delaying deletion of archived data on HCP even if the primary XVL is deleted. In HNAS version 12.1 and higher, the HCP no delete feature sets a retention on the object for a user-defined interval in the future, after which the disposition service will eventually delete it.

If an XVL is accidentally deleted that represents a file that has been uploaded to HCP by Data Migrator to Cloud and no instance of the XVL exists in an HNAS file system snapshot, HCP retains the object in its namespace for a user-defined period of time rather than issuing the purge. If the accidental deletion is recognized in time, the file can be retrieved manually from HCP back to the HNAS file system. The decision whether to purge or retain a file upon deletion of the XVL depends on the presence of a retention class in the HCP namespace. After the retention period expires, the HCP disposition service will automatically clean up these files from the namespace.

HCP no delete functionality

To use this feature, create a retention class on HCP for the target namespace.

HNAS sets the retention to the specified offset instead of deleting the object.

1 - 1 of 1 Namespaces

The screenshot shows the HNAS web interface. At the top, there's a navigation bar with 'Name', 'Object Count', 'Alerts', 'Storage Used', and 'Quota'. Below that, a breadcrumb trail shows 'Overview', 'Policies', 'Services', 'Compliance', 'Protocols', 'Monitoring', and 'Settings'. The main content area is titled 'Retention Classes' and shows a 'Privileged Delete' page. A modal dialog box titled 'Create Retention Class' is open. It has the following fields: 'Retention Class Name' (HNAS), 'Description' (retain deleted files for an additional 6 months after deletion), 'Retention Method' (Offset), and a checkbox for 'Allow Disposition service to delete objects when expired' which is checked. There are input fields for 'Years', 'Months' (6), and 'Days'. At the bottom right of the dialog are 'Create Retention Class' and 'Cancel' buttons.

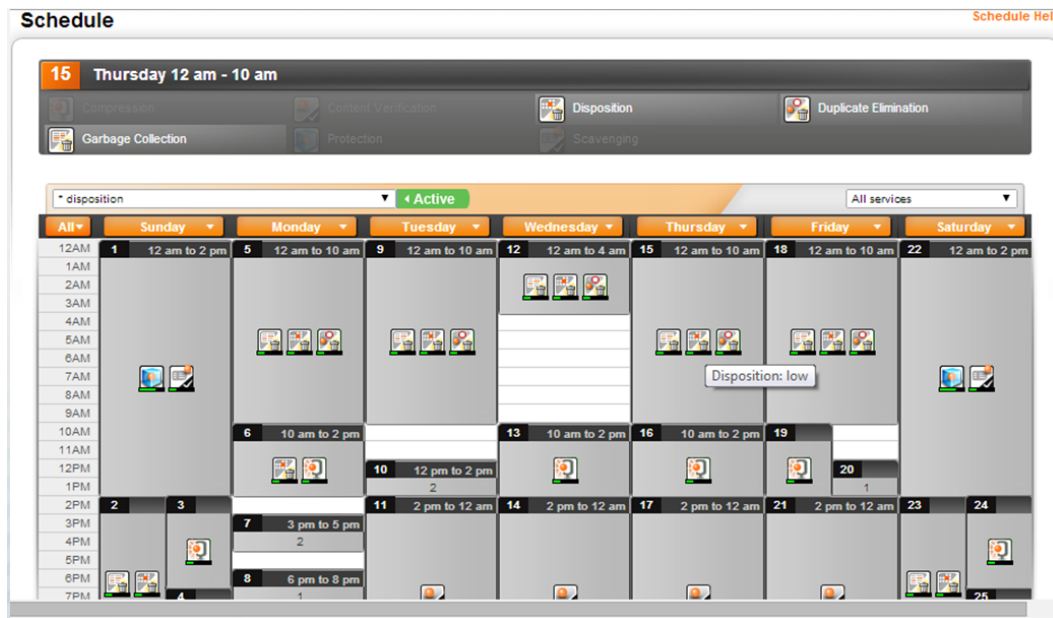
Note: This is not the default retention setting. Default retention setting deletes the object after a certain interval. The HCP no delete feature sets a retention value on HNAS in the place of deleting the object.

When the retention class is created and an XVL is deleted on HNAS (or last snapshot ages out), Data Migrator to Cloud will set the retention value on the object on HCP. You have that period to retrieve file from HCP if deletion was accidental. The next figure gives an example of the retention timeframe.

Contents of: bt03/hcpbua0/FBA5312E6F82D880000000000000000/hcpbua0/9B3P

Name	Owner	Domain	Size	Retention	Retention Class	Ingested
wfile-corrupt-ecc.cpp.18890.1529039	bt03		4083	11/22/2014 9:59AM		5/22/2014 9:56AM
WfsCacheInvalidationSuppressor.cpp.18857.1...	bt03		4042	Deletion Allowed		5/22/2014 9:56AM
p.FsbLoadStatistic.cpp.18896.1529039	bt03		40	Deletion Allowed		5/22/2014 9:56AM
s.post.cpp.18809.1529038	bt03		14078	Deletion Allowed		5/22/2014 9:56AM
s.find-uint32-on-disk.cpp.18765.1529038	bt03		22094	Deletion Allowed		5/22/2014 9:56AM
s.filesystem-remake-tiers.cpp.18820.1529038	bt03		4371	Deletion Allowed		5/22/2014 9:56AM
s.Commands.cpp.18806.1529039	bt03		33914	Deletion Allowed		5/22/2014 9:56AM
s.inquiryIdentifierBase.cpp.18773.1529039	bt03		6636	Deletion Allowed		5/22/2014 9:56AM
s.WfsCommandBase.fwd.cpp.18816.1529039	bt03		836	Deletion Allowed		5/22/2014 9:56AM
s.frametocap.cpp.18782.1529038	bt03		11360	Deletion Allowed		5/22/2014 9:56AM
WfsOperation.cpp.18684.1529038	bt03		11286	Deletion Allowed		5/22/2014 9:56AM
DSBSnapshotCheckpointList.cpp.18777.1529039	bt03		1840	Deletion Allowed		5/22/2014 9:56AM
wfs_lru_move.cpp.18888.1529039	bt03		5588	Deletion Allowed		5/22/2014 9:56AM
p.WfsWellKnownObjectNumbers.cpp.18705...	bt03		38	Deletion Allowed		5/22/2014 9:56AM

The HCP Disposition service periodically runs to delete files for which the retention period has expired so that they do not remain permanently on HCP.



The HCP log will show disposition running and how many files it purged.

Hitachi Content Platform User > btenant03n

Overview Namespaces Services Security **Monitoring** Log Out / Password

Tenant Events

All Events expand all Items 20

User	Severity	Date	Event
btenant03n	Notice	2/4/2014 2:24PM	User authenticated
[internal]	Warning	2/4/2014 2:24PM	Password is invalid
btenant03n	Notice	2/4/2014 1:57PM	User authenticated
[internal]	Notice	2/4/2014 1:51PM	Disposition service stopped: run complete
[internal]	Notice	2/4/2014 1:51PM	Disposition service stopped: run complete
User ID: 1			
Event ID: 2087 Disposition service stopped: examined 10 object(s), deleted 1. Tenant: btenant03			
btenant03	Notice	2/4/2014 1:48PM	User authenticated
btenant03n	Notice	2/4/2014 1:40PM	User account updated
[internal]	Notice	2/4/2014 1:24PM	Disposition service stopped: run complete
[internal]	Notice	2/4/2014 1:24PM	Disposition service stopped: run complete
btenant03n	Notice	2/4/2014 1:19PM	User account updated
btenant03n	Notice	2/4/2014 1:19PM	Namespace updated
btenant03n	Notice	2/4/2014 1:19PM	User authenticated
btenant03	Notice	2/4/2014 1:18PM	User account created

Chapter 4: Overview of Hitachi NAS Universal Migrator

The Hitachi NAS Universal Migrator allows data to be migrated from file systems on pre-existing, third-party NAS systems to HNAS systems. Clients can continue to access and use the data while the migration is in progress. This means that data stored on a third-party NAS system is immediately available for access, via an HNAS system. File systems from the third-party NAS system can be actively used, with HNAS as the frontend, while the data migration is in progress. The Universal Migrator provides fast migration of large amounts of data, while also allowing the use of the data, during migration, with minimal down time (compared to previous types of NAS migration).

It does this in two stages or phases. The first virtualization stage discovers data on the LNAS source and creates objects on the HNAS file system. The second migration stage copies the user data from the original file system so that at the end all data is wholly contained on the HNAS file system. At that point the original NAS can be disconnected.

Overview of Universal Migrator Capacity Based (UMC) license

Before you can use Universal Migrator, the Universal Migrator Capacity (UMC) license must be installed. If you do not have a license key, contact customer support.

The Universal Migrator Capacity license:

- Is based on total capacity in TBs for all virtualized file systems across the cluster.
- Is fixed at the discovery phase of each association.
- Periodically checks the total licensed capacity against the recorded size of all the virtualized associations. Once the initial virtualization of associations has completed, the only reason for a change in the actual licensable capacity would be:
 - The addition of new associations (increase).
 - The removal of existing associations (decrease).
 - The conversion of a virtualized association to a migration association (decrease).

Universal Migrator Capacity License considerations

- License capacity is based on total capacity in TBs for all virtualized file systems across the cluster.
- For license purposes the capacity of each association is fixed at the discovery phase.
- If the limit is reached or exceeded, warning messages will be generated periodically and further associations will be blocked.
- The following command lists each virtualization path along with the number of bytes that path has virtualized. The paths are grouped by file system. Virtualization paths that are in migration mode will report a virtualization usage of 0.
 - `virtualization-license-report`

Universal Migrator Capacity event notification

You will receive an event notification when virtualization exceeds the following thresholds:

- 9220 is an informational event notification when virtualization exceeds 80 percent of the license allowance.
- 9221 is a warning event notification when virtualization exceeds 95 percent of the license allowance.
- 9222 is a severe event notification when virtualization exceeds 100 percent of the license allowance.

Hitachi NAS Universal Migrator Terms

Refer to the following list of terms used for the Hitachi NAS Universal Migrator.

- Association - The configured connection between a mount point on the LNAS and a directory in a file system on the NAS. An association is also referred to as a virtualization path.
- Excluded directories - The user-defined list of directories that will not be created on the virtualized file system.
- NAS - The Hitachi Vantara NAS system that will hold the data, after migration.
- IngestedFile - An object (directory or file) in the NAS file system that is in the process of being virtualized or migrated. As such, it contains extra metadata (compared to a regular file/directory), but incomplete or absent user data. In some ways (principally user data read/write access) an **IngestedFile** can be thought of as behaving similarly to an XVL. The extra metadata is necessary for two reasons:
 1. To keep track of the current virtualization/migration state of the file.
 2. To maintain a link to the LNAS version of the file.
- LNAS - The pre-existing "legacy" NAS system that holds the data to be migrated.
- Migration - The process of bringing user data for an object from the LNAS to the NAS.

- Regular file/directory - The normal type of object (a file or directory) in the NAS WFS file system.
- Virtualization - The process of discovering an object on the LNAS, and creating an IngestedFile to represent the LNAS object in the file system.
- XVL - External cross volume link.

Pre-migration considerations for Hitachi NAS Universal Migrator

This section describes the pre-migration considerations for Hitachi NAS Universal Migrator.

Number and layout associations

The Universal Migrator is designed to deal with multiple associations per file system, concurrently; however, due to fundamental file system limitations, the simplest management is attained by configuring only one association per file system, mapped to a directory in the root of the file system.

NFS export on the LNAS used by HNAS

The export from the LNAS should have the following options set: `rw`, `sync`, `no_subtree_check`, `no_root_squash`. These options allow the HNAS to fully control the data and metadata of the files and directories. The export must also be configured to only allow access to the HNAS, as if other clients are able to access the data with `rw` and `no_root_squash`, then the HNAS's view of the data will not be consistent, and it will lose track of what has been virtualized or migrated. This could result in data loss.



Note: If you are restricting the LNAS access on a per-IP basis on the export, include all IP addresses that an EVS can utilize.

The export should only contain real (not virtual) file systems. Examples of virtual file systems are directories such as `/dev` or `/proc` on a Linux server, or `/.snapshot` on a NAS device. It may be difficult or impossible to exclude `/.snapshot`, or similar, via the LNAS configuration. In this case the directory should be excluded at the HNAS using the `virtualization-path-excluded-directory-*` commands. The HNAS file system uses its storage resources in different ways to the LNAS; therefore, you cannot depend on the space being used being identical on each. Furthermore, during the process of virtualization and migration, the HNAS file system needs to use extra storage space to track the state of the processing.

The following arrangements on the LNAS should be avoided, as they will lead to unpredictable behavior.

1. Nesting or overlapping exports on the LNAS used for associations.
2. Hard links across multiple LNAS exports.

Export/shares from HNAS

It is recommended not to set `no_root_squash` in NFS exports. This prevents accidental modification of the file system objects that track the state of the association.

Backup and replication policies, disaster recovery

This section describes backup and replication policies and disaster recovery.

Virtualization

During virtualization the LNAS is the canonical store of the data. To ensure that there is no loss of data, if the live file system is damaged, it is necessary for backups/replications/snapshots to be configured on the LNAS. System administrators should ensure that they have sufficient backups/snapshots of the LNAS data set before connecting the HNAS.

While it is not necessary to have backups or replications configured for the HNAS during virtualization (because they would not contain any data that was not recoverable through the LNAS backup), it is recommended to configure these when the association is created. This reduces the risk of forgetting to start (or not knowing when to start) them when migration begins. It also allows time to be sure that everything is working correctly. Incremental backups/replication schedules started in the virtualization phase will pick up data added during the migration phase. When replicating during the virtualization phase, a message will appear in the replication log stating that "ingested files are excluded from this operation". This is normal.

In the event that recovery from a backup is required during the virtualization phase, the simplest course of action is listed below.

1. Prevent client access.
2. Delete the association, then remove all of the files/directories it created from HNAS. If the association was in the root of an HNAS file system, it is recommended that you format the file system after deleting the association. Use `virtualization-delete-path --force` command.
3. Recover the LNAS from backup.
4. Recreate the association.
5. Start the virtualization.
6. Allow client access.

Migration

During migration, some data is on HNAS only, while other data is on the LNAS only. This makes backups/replications and subsequent recovery more complicated, and depends on the replication/backup mechanism that is used.

Ideally, the replication/backup of data on the HNAS and LNAS would be synchronized, such that the data contained in the pair of backups is guaranteed to be consistent. A consistent set could be guaranteed by the following method:

1. Prevent client access to the data.
2. Pause the migration by issuing the `virtualization-path-control --pause` command.
3. Wait for activity to stop by issuing the `virtualization-path-list` command and wait until the counts displayed in the list stop changing.
4. Take snapshots of the LNAS and HNAS and start the backup/replications of these snapshots.
5. Allow client access.

This method can, however, be undesirable because you must prevent client access. A more acceptable alternative is to have time synchronized snapshots of the HNAS and LNAS to use for the replication/backups. This runs the risk of having inconsistencies between the LNAS and HNAS. You could mitigate this by pausing the background processes and/or ensuring the backups are done at a quiet time for client access.

HNAS NDMP file replication and tape backups

Because object-based backup is incompatible with virtualization, file based replication must be used. The recovery of data from the HNAS backup, following damage to the live HNAS file system, has to encompass a manual merge of the LNAS and HNAS data. This is necessary because, although the IngestedFiles contained in the backup are preserved, the associated metadata is lost because it does not form part of the NDMP backup. The result is that, although the user data of migrated files and the directory structure that contained them will recover intact, the connection of this directory structure to the LNAS is not easily remade.

The sequence to recover, if NDMP replications or backups are used, is as follows:

Procedure

1. Prevent client access.
2. Delete the association (if it has not been lost in the file system damage).
3. Recover HNAS data to a location other than that which will be used for the association.
4. If necessary, recover LNAS data.
5. Recreate the association and allow virtualization to complete.
6. There are now two sets of files, those recovered from the LNAS and virtualized, and those that were previously migrated and have been recovered to a separate location. Depending on the volume/type of files that are in the latter set, and how many renames/moves have happened, you can do either of the following:
 - a. Examine the files manually and copy the migrated files into the virtualized directory structure, file by file, depending on some case-specific judgment.
 - b. Use an automated method (rsync/robocopy) to move the migrated files into the virtualized directory structure.
7. Allow client access.

Setting up LNAS and HNAS for virtualization

Before using the Hitachi NAS Universal Migrator, you must prepare the systems by associating the HNAS to the LNAS. The following steps describe this process. Note that your preparation must use the device names and IP addresses of your actual system.

Assuming a legacy NAS device with hostname LNAS at IP address 192.168.1.1, exporting a directory `existing_data_dir` as `existing_export` using NFSv3. The LNAS is configured such that a sub directory `.snapshot` exists in the root of `existing_data_dir`, to allow browsing of snapshot data.

Procedure

1. Create a file system, `<hnasfs>`, using storage appropriate to contain the data set to be migrated from the LNAS.
2. Create NFS exports to the file system, and any other HNAS configuration, as necessary. The directory on the HNAS file system that will be the root of the association must be empty.

If you want to create exports within the root of the association, uncheck the **Create path if does not exist** checkbox on the SMU. If you use the CLI, use the `nfs-export add` command with the `-i` and `-d` (DONTCREATE) options for example, `nfs-export add -i -d source_root/data1 FS1 /source_root/data1`. This will ensure the root of the association remains empty until the virtualization starts.

3. Add a new IP address to the LNAS, which the HNAS will use for the migration (assuming the LNAS's existing IP address will move to the HNAS when it is introduced into the environment).
4. Create the association, `<assoc1>` at the HNAS console, using the following commands:

```
virtualization-path-create -t <hnasfs> -n <assoc1> -s nfs://lnas/
existing_export
```

This can be modified if necessary using the following command:

```
virtualization-path-modify
```



Note: This command cannot be used after issuing:

```
virtualization-path-control -t <hnasfs> -n <assoc1> --
start
```

When the association has been created, `virtualization-path-list` will show `Seen Dirs` as 1, which is the root of the LNAS export.

5. Add the `.snapshot` directory to the list of excluded directories for the association:

```
virtualization-path-excluded-directory-add -t <hnasfs> -n
<assoc1> -d .snapshot
```

Again, this can be changed (`virtualization-path-excluded-directory-list`, `virtualization-path-excluded-directory-delete`) up to the point that `virtualization-path-control -t hnasfs -n assoc1 --start` is used.

6. Prevent any further client access to the LNAS by renaming, or otherwise changing, the export. Ensure that existing export NFSv3 export is configured on the LNAS in such a way as to meet the suggested best practices. At this point all other methods for clients to directly connect to the LNAS should be disabled (for example, CIFS shares).
7. If necessary, transfer IP addresses from the LNAS to the HNAS (apart from the one created in step 4).

Starting virtualization

When starting virtualization, you have two options. You can:

- Stop at the end of the virtualization phase, and do not migrate any data.
- Automatically start migrating data once virtualization is complete.

Procedure

1. Start the virtualization.
 - a. If you want to stop at the end of the virtualization phase, and not automatically migrate any data, use the following command:


```
virtualization-path-control -t hnasfs -n assoc1 --start
```

Wait for the virtualization to complete. This has the benefit that, at any time, the HNAS can be removed and you can revert back to using the LNAS, without having to reconstruct the data. The disadvantage of this is that the file system performance (seen by clients) will be significantly degraded while in virtualization mode.
 - b. To start the data migration, use the command, `virtualization-path-control -t hnasfs -n assoc1 --migrate` immediately after using `virtualization-path-control -t hnasfs -n assoc1 --start`. The *advantage* is that the client access (for files) will automatically transition out of the poorly performing virtualization mode as soon as possible. It should be noted, however, that until the association is deleted and all objects are converted into TitanFile objects (that is, identical to objects that were only ever created on the HNAS outside of an association), the performance will not match that of a "normal" HNAS WFS file system. This is because it is only at this point that the requests by clients against the objects can be completely served in hardware. This has the *disadvantage* that, if you wish to revert back to using the LNAS on its own, you would have to manually recombine the data that is held on the HNAS with that on the LNAS.
2. Once the virtualization has been started, it is possible for clients to access the data on the LNAS via the HNAS. This would normally be achieved by creating NFS exports and/or CIFS shares for `hnasfs` in such a way as to make the data available at the same location the clients were previously accessing: `lnas:/existing_data_export`. This also requires changing the configuration that is external to the HNAS, for example, DNS records and/or client mount points.
3. Monitor progress of the virtualization/migration.
4. Use `virtualization-path-list -t hnasfs` to display information about the association, including the counts of objects in various states.

5. Events related to the association are raised in the event log. For example:

Information: The virtualization path to filesystem hnasfs, association name assoc1, from URI nfs://lnas/existing_data_export has been created.

Information: The status of the virtualization path to filesystem hnasfs, association name assoc1, has been modified: Virtualization has started.

Information: The virtualization phase of filesystem hnasfs, association name assoc1 completed.

Information: The status of the virtualization path to filesystem hnasfs, association name assoc1, has been modified: Migration has started.

Information: The migration phase of filesystem hnasfs, association name assoc1 completed.

Information: The virtualization path to filesystem hnasfs, association name assoc1, has been deleted.

6. If you chose not to automatically proceed with virtualization, you can issue **virtualization-path-control -t hnasfs -n assoc1 --migrate** at any time, either before or after virtualization has completed. This prevents any further client access to LNAS. You must first ensure that `existing_export NFSv3 export` is correctly configured on the LNAS.
7. Once migration has completed, you need to delete the association `virtualization-path-delete -t hnasfs -n assoc1`.

Monitoring the association

The **virtualization-path-list** command can be used to display the state of associations. This includes a count of the file system objects in the association that are in various states. While this provides a good overview of the progress of the association, it may occasionally be unclear, especially when the association has been paused and restarted or when connection to the LNAS has momentarily been lost, and the HNAS is automatically recovering. Events are recorded in the event log when associations are created or deleted, and when the virtualization and migration phases complete.

Incompatible features

It is not possible to successfully object replicate a file system containing associations.

Performance Limitations

Once migration is complete, the performance when accessing data in the target file-system is that of a normal HNAS file system.

During the virtualization phase the performance is governed by a number of factors, including the capability of the LNAS, and the network connection to it. In addition the HNAS has to track the state of the objects in the association and send all modifying and IO operations to the LNAS. The result of this is that performance compared to a normal HNAS file system is significantly degraded. This is particularly the case when many (several hundred) parallel client operations are made on the virtualized data at the exact same time. If the desired use case of the feature is likely to include this type of load, it may be prudent to postpone widespread client access until after virtualization is complete, and migration is well underway.

Upgrade and downgrade considerations

Any associations should be removed using the `virtualization-path-delete` command.

- If in virtualization mode, the association can be deleted.
- If part way through migration, it is best to wait until migration completes, and then delete the association. Data will be recovered onto the HNAS, rather than being in two different places.

Troubleshooting Hitachi NAS Universal Migrator

This section provides common problems and solutions.

Cannot create associations

Cannot create associates, as the remote server is inaccessible. For example:

```
mercury2n3(HNAS-4100):$ virtualization-path-create -t HNASfs -n
demo_assoc -s nfs://mercuryc5/LNAS
```

```
Create virtualization path failed: The remote server is inaccessible
```

```
Additional information: NFS Status: RemoteTimeout
```

```
[virtualization-path-create took 30 s.]
```

- Try with IP address rather than hostname, and/or check the DNS settings of your network.
- Use `remote-nfs-exports` on the HNAS console to show what exports are available to the HNAS from the LNAS.

Hitachi NAS Universal Migrator associations paused

When using the `virtualization-path-control` command, the pause completes successfully, but the counts shown by the `virtualization-path-list` command are still seen to change.

This is because it is necessary to complete processing the objects that are currently being operated on before stopping work. If a directory is being virtualized that contains many entries, this may take some 10s of seconds.

Virtualization or migration does not complete

Procedure

1. Check the `virtualization-path-list` command to see if there are any failed files.



Note: The `virtualization-path-files` command could take some time to complete.

2. Check the event log. The migration may not have completed due to insufficient space on HNAS, in which case it will pause and there will be no failed files.
3. If step 1 shows failed files, identify the problematic files with the `virtualization-path-files` command.
 - a. `virtualization-path-files` Inspect the files on the LNAS to ensure that they are correct in that file system.
 - b. Use `remote-nfs-errors` to gain insight as to why they may have failed.
 - c. `virtualization-path-files --list-failed` may just show "/" (that is, root).
4. Fix problems, if they are not obvious, then the following strategies should allow you to continue.
 - a. For failed files during virtualization, move the failing file out of the exported directory on the LNAS. Manually copy it over to the HNAS.
 - b. For failed files during migration, remove the failing file from the HNAS. Manually copy the LNAS version of the file over to the HNAS.
5. Once you think that you have fixed the problems use the `virtualization-path-files` command to retry the failed files.

It is recommended that if it is only virtualization that has failed and migration has not been started, it may be simplest to delete the virtualization path and start again - all data is still contained on the LNAS at this point.

Hitachi NAS Universal Migrator Console Commands

This section lists the Hitachi NAS Universal Migrator console commands. See the man pages for more details about a specific command options.

virtualization-license-report CLI command

Lists the amount of data currently virtualized by all virtualization paths.

virtualization-path-control CLI command

Controls the background processing of files for the virtualization path for the specified target vivol/volume.

virtualization-path-create CLI command

This command creates a virtualization path association between a remote NFS export source and a local file system, vivol or directory target.

To ensure data can be managed correctly between the Legacy NAS and the HNAS, it is recommended that the mount on the Legacy NAS is exported with `rw, sync, no_subtree_check, no_root_squash`. It is also advised that, due to `no_root_squash`, the mount is available only to the HNAS.

virtualization-path-delete CLI command

This command deletes a virtualization path association between a remote NAS NFS export source and a local file system or vivol target.

virtualization-path-excluded-directory-add CLI command

This command adds an excluded directory to the virtualization path association between a remote NFS export source and a local file system, vivol or directory target.

This command can be applied while the association has created, but the virtualization has not been started.

virtualization-path-excluded-directory-delete CLI command

This command deletes an entry from the list of directories to be excluded from the virtualization path association between a remote NFS export source and a local file system, vivol or directory target.

This command can only be applied once the association has been created but the virtualization has not yet started.

virtualization-path-excluded-directory-list CLI command

This command shows a list of the excluded directories registered to the virtualization path association between a remote NFS export source and a local file system, vivol or directory target.

virtualization-path-files CLI command

This command lists all files and directories that have failed to virtualize correctly. It allows these to be retried as well. Retries, for individual files, can also be achieved by requesting them as normal, through an 'ls' command.

virtualization-path-journal-control CLI command

This command manages journal of files deleted from remote server for a virtualization path association.

virtualization-path-journal-show CLI command

This command displays a journal of files deleted from remote server for a virtualization path association.

virtualization-path-list CLI command

This command lists all NAS virtualization path associations defined for the specified file system or for all file systems if the -a or --all option is used.

virtualization-path-modify CLI command

This command changes the source URI associated with a pre-existing virtualization path that is mapped to a local file system, vivol or directory target.

This command will change the location that data is received from when scanning for entries to virtualize. After virtualization process has started changes by virtualization-path-modify command are no longer allowed. To change the source in such case the virtualization path needs to be deleted and created again.

virtualization-path-stats CLI command

This command displays statistics associated with NAS virtualization paths, detailing the amount and time taken by the migration since the statistics were last reset, or start-up, whichever is the most recent.

Control via SMU GUI

At the time of writing there is no GUI support for the feature.

Formatting file systems



Caution: Formatting a file system from the CLI that contains a virtualization path will prompt you to delete the virtualization path. However, if the SMU is used to format a file system that contains a virtualization path, there will be no prompt. Therefore, it is important to remember to delete the virtualization path for a file system before formatting through the SMU.

Appendix A: Creating specific and detailed migration rules

Before building migration rules, refer to the following information regarding syntax, keywords, connectors, conditionals, and statement order. The following example provides a three-step process for assembling simple, yet specific and detailed rules:

1. Start with a simple INCLUDE statement that is specific about what should be migrated, such as:

```
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)
```

2. Refine the INCLUDE statement by adding exceptions to the rule with restrictive EXCLUDE statements. Add these EXCLUDE statements above the INCLUDE, such as:

```
EXCLUDE (<FILE_SIZE_UNDER 2MB>)
```

```
EXCLUDE (<ACTIVE_WITHIN 14>)
```

3. The rule should finally appear this way:

```
EXCLUDE (<FILE_SIZE_UNDER 2MB>)
```

```
EXCLUDE (<ACTIVE_WITHIN 14>)
```

```
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)
```

Click on a topic at the left for more information about a specific rule.

Rules syntax

Data migration rules compare a series of INCLUDE and EXCLUDE statements, each qualified by expressions stating the criteria for data migration. The following guidelines govern rule building:

- **At least one INCLUDE or EXCLUDE.** Each rule must contain at least one INCLUDE or EXCLUDE statement. Rules consisting only of EXCLUDE statements imply that everything on primary storage should be migrated except what has been specifically excluded.



Note: If a rule contains only INCLUDE statements, all items not specified by the INCLUDE statements are excluded.

- **Wildcards.** The asterisk (*) can be used as a wildcard character to qualify PATH and FILENAME values.
 - When used in a PATH value, “*” is only treated as a wildcard if it appears at the end of a value; for example, <PATH /tmp*>.
 - In a FILENAME value, a single “*” can appear either at the beginning or the end of the value.
 - Multiple instances of the wildcard character are not supported and additional instances in a value definition will be treated as literal characters.
- **Bracketed keyword/value pairs.** Expressions identifying migration criteria should be enclosed in brackets. All criteria contain a keyword, defining the condition for data migration, followed by a single value of a list of values; for example, <FILENAME *.doc>.
- **Evaluation of statement sequence.** When using multiple INCLUDE or EXCLUDE statements, they are evaluated using top-down ordering.
- **Grouping criteria within statements.** Parentheses are used to group the criteria in INCLUDE and EXCLUDE statements; for example, INCLUDE (<PATH /Temp/*>).
- **Number of INCLUDE or EXCLUDE statements per line.** When using multiple INCLUDE or EXCLUDE statements in a rule, each INCLUDE or EXCLUDE statement must be placed on its own line (multiple INCLUDE and/or EXCLUDE statements may not be put on the same line).
- **Separating multiple listed values.** When defining multiple values in a FILENAME list, use a comma to separate values; for example, INCLUDE (<FILENAME *.mp3,*.wav,*.wmv>).
- **Characters requiring escaping.** the following characters need to be escaped with a backslash (\) when used as a part of PATH or FILENAME values: \ (backslash), > (greater than), and , (comma); for example, INCLUDE (<FILENAME *a\,b> OR <PATH /tmp/>ab>).



Note: Backslashes used when specifying a domain and user name should **not** be escaped (double backslashes are not required when specifying domain_name\user_name).



- **Forward slash (/) reserved as a path separator.** The forward slash (/) is used as a path separator; as such, it must not be used in a FILENAME list.

- **Evaluation of absent PATH.** If a PATH element is not specified in a statement, the statement will apply to the entire file system or virtual volume defined in the data migration path.
- **Quotation mark usage.** Quotation marks (") are not allowed around a FILENAME or PATH list.

Keywords

The following table describes the keywords and their related values that can be used to build rule statements. Each keyword can be defined in the rule with an INCLUDE or EXCLUDE statement to indicate how the keyword values are to be applied.

Keyword	Value(s)
FILENAME	<p>Names and types of files contained in the rule. Separate multiple names by commas. FILENAME values may start or end with a "*" wildcard character to indicate all files starting/finishing with specific characters.</p> <p>Usage:</p> <p>FILENAME will often be used with an INCLUDE statement to ensure that non-essential files are migrated to secondary storage. It can also be used with an EXCLUDE statement to prevent specific important data sets from being migrated.</p> <p>For example:</p> <pre><FILENAME *.mp3,*.txt,*filename, filename*></pre>
PATH	<p>Specifies literal paths to which a rule applies. Values must be full paths, starting with a forward slash (/). Separate multiple paths by commas. PATH values may end with a "*" wildcard character to indicate all subdirectories under the specified path.</p> <p>Usage:</p> <p>When used in an INCLUDE statement, PATH specifies directories to migrate. This is useful when migrating less-critical directories such as temp or home directories. When used in an EXCLUDE statement, directories can be excluded from migration, leaving all the files within on primary storage.</p> <p>For example:</p> <pre><PATH /temp/*,/home*/other/dir*></pre>
USERNAME	<p>Specifies user names to which a rule applies. Values must be valid Windows or UNIX user names. Separate multiple names by commas.</p> <p>Usage:</p>

Keyword	Value(s)
	<p>When used in an INCLUDE statement, USERNAME specifies the user name of file owners whose files are to be migrated. This is useful when migrating files owned by a particular user. When used in an EXCLUDE statement, users can be excluded from migration, leaving all the files owned by the specified user(s) on primary storage.</p> <p>Windows user names are specified in the form domain\username.</p> <p> Note: Backslashes in user names should not be escaped (double backslashes are not required). For example: jjames, myco\smithr, myco\wsmith</p> <p> Note: The USERNAME keyword is not supported for cloud data migration rules.</p>
FILE_SIZE_OVER	<p>Identifies a subset of files in a rule with sizes crossing an upper threshold. The threshold value is appended to the keyword and defined by the threshold size in B, KB, MB, or GB.</p> <p>Usage:</p> <p>This will likely be used with INCLUDE statements to ensure files of very large sizes are migrated to secondary storage.</p> <p>For example:</p> <p><FILE_SIZE_OVER 4GB></p>
FILE_SIZE_UNDER	<p>Identifies a subset of files in a rule with sizes crossing a lower threshold. The threshold value is appended to the keyword and is defined by the threshold size in B, KB, MB, or GB.</p> <p>Usage:</p> <p>This will usually be used in an EXCLUDE statement to ensure that very small files are not migrated en masse. Migrating small files that take up little space provides minimal value in extending the efficiency of primary storage.</p> <p>For example:</p> <p><FILE_SIZE_UNDER 10KB></p>
OLDER_THAN	<p>Identifies files that were created more than a specified number of days in the past (files older than x days). The value is appended to the keyword and defines the number of days within which the activity has occurred from the current date and time</p> <p>Usage:</p> <p>Used primarily in INCLUDE statements to ensure that older files are migrated.</p>

Keyword	Value(s)
	For example: <OLDER_THAN 28>
NEWER_THAN	Identifies files that were created less than a specified number of days in the past (files newer than x days). The value is appended to the keyword and defines the number of days within which the activity has occurred from the current date and time. Usage: Used primarily in EXCLUDE statements to ensure that newer files are not migrated. For example: <NEWER_THAN 14>
INACTIVE_OVER	Identifies files that have not been accessed within a specific number of days. A file's last access time is updated whenever the file is read or modified. The value is appended to the keyword and defines the number of days of inactivity from the current date and time. Usage: Used primarily in INCLUDE statements to ensure that older, less frequently used files are migrated. For example: <INACTIVE_OVER 21>
ACTIVE_WITHIN	Identifies files accessed within a specific number of previous days. A file's last access time is updated whenever the file is read or modified. The value is appended to the keyword and defines the number of days of inactivity from the current date and time. Usage: Used primarily in EXCLUDE statements to prevent actively used files from being migrated. For example: <ACTIVE_WITHIN 30>
UNCHANGED_OVER	Identifies files not modified within a specific number of previous days. A file's modification time is updated whenever the file's contents have been changed. The value is appended to the keyword and defines the number of days of inactivity from the current date and time. Usage: Used primarily in INCLUDE statements to ensure that older, less frequently used files are migrated.

Keyword	Value(s)
	For example: <UNCHANGED_OVER 14>
CHANGED_SINCE	Identifies files modified within a specific number of previous days. A file's last access time is updated whenever the file's contents have been changed. The value is appended to the keyword and defines the number of days of inactivity from the current date and time. Usage: Used primarily in EXCLUDE statements to prevent actively used files from being migrated. For example: <CHANGED_SINCE 7>

Connectors

Statements can combine multiple criteria, as follows:

- **AND** indicates that both statements must be satisfied. For example, in the statement:

```
INCLUDE (<FILENAME *.mp3> AND <FILE_SIZE_OVER 5GB>)
```

both conditions must be true in order for the statement to be true.

- **OR** indicates that only one statement needs to be satisfied. For example, for the same statement, replacing AND with OR:

```
INCLUDE (<FILENAME *.mp3> OR <FILE_SIZE_OVER 5GB>)
```

only one condition needs to be true for the statement to be true.

While **AND** requires both conditions to be true, **OR** only requires that either condition to be true.

Conditionals

The following table shows a set of rules with explanations. The syntax can easily be broken down into cause and effect statements, identified by IF and THEN connectors.

Rule	Description
INCLUDE (<FILENAME *.doc>)	IF the file is a .doc file, THEN include it for migration.

Rule	Description
EXCLUDE (<PATH /mydir/*>)	IF the path is the /mydir directory THEN exclude it from migration.
INCLUDE (<FILENAME *.prj> AND <FILE_SIZE_OVER 4GB>)	IF the file is a .prj file AND the .prj file is over 4 GB in size, THEN include it for migration.
INCLUDE (<PATH /unimportant>)	IF the path is the /unimportant directory THEN include it for migration.
EXCLUDE (<FILE_SIZE_OVER 100GB>) INCLUDE (<FILE_SIZE_OVER 12GB>)	IF files are larger than 12 GB but smaller than 100 GB in size, THEN include them for migration.

Statement order

Statement order is critical. Statements are evaluated top-down, starting with the first statement defined. Therefore, as the following examples illustrate best practice usually specifies EXCLUDE statements at the top of the rule.

Rule scenario A:

```
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)
EXCLUDE (<ACTIVE_WITHIN 14>)
EXCLUDE (<FILE_SIZE_UNDER 2MB>)
```

The above rule is interpreted as:

- IF path name includes /Temp **AND** file name is *.mp3 THEN MIGRATE.
- IF file is active less than 14 days **AND** less than 2 MB in size THEN EXCLUDE.

In scenario A, all the .mp3 files under /Temp will be migrated based on the first INCLUDE statement. Statements 2 and 3 are disregarded since they are evaluated after the more inclusive INCLUDE statement that has already added what rules 2 and 3 are trying to exclude.

Rule scenario B:

If the same rules were ordered differently:

```
EXCLUDE (<FILE_SIZE_UNDER 2MB>)
EXCLUDE (<ACTIVE_WITHIN 14>)
INCLUDE (<PATH /Temp> AND <FILENAME *.mp3>)
```

The above rule is interpreted as:

- IF file is less than 2 MB in size OR active less than 14 days THEN EXCLUDE.
- IF path name includes /Temp AND file name is *.mp3 THEN MIGRATE.

In this scenario, only .mp3 files greater than 2 MB in size that have been inactive for greater than 14 days will be migrated.

Appendix B: Configuring management ports for Data Migrator to Cloud

Best practice is to use the aggregate ports instead of the management ports. Aggregate ports transfer data with a higher outgoing performance rate. However, if you plan to use the management ports for cloud targets, you must define the following:

- DNS
- Networking



Note: The Virtual Secure Servers feature is not compatible with Data Migrator to Cloud.

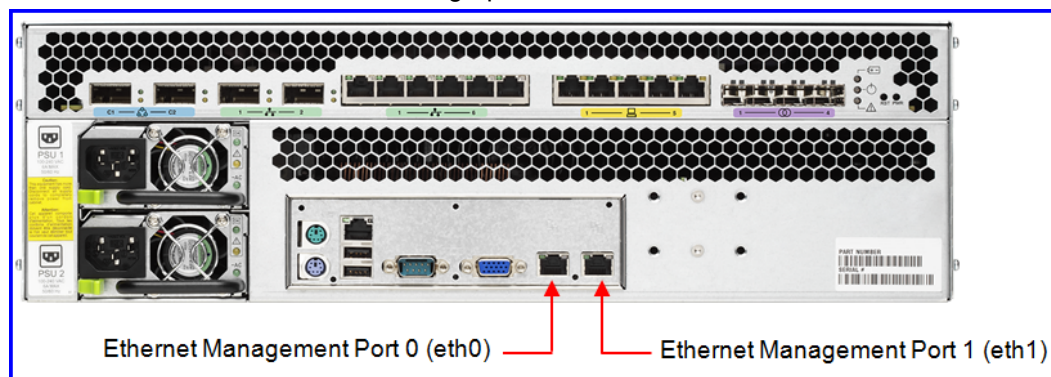


Caution: Before using Data Migrator to Cloud, you must ensure that the managements ports are properly configured.

Data Migrator to Cloud connects to the cloud through one of the management ports on the system and not through the aggregate ports that are used for NFS or CIFS access. Because of this, you must configure the eth0 or eth1 network interface card with an IP address, netmask, and gateway that is routable to the cloud target.

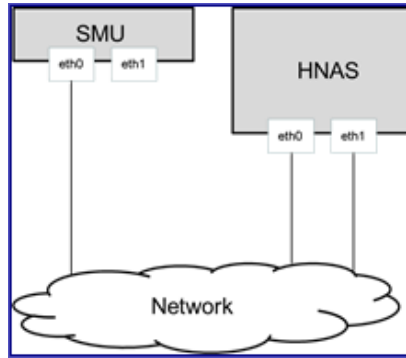
- If the cloud target is Hitachi Content Platform, a route must exist to the namespace that will be configured as part of the cloud account.
- If the cloud target is Amazon S3, a route must exist to <https://s3.amazonaws.com/>.

In a clustered environment, usually one network interface card is configured for the cluster interconnect (eth1) and the other (eth0) is not configured. In general, the cluster interconnect is a private network among the cluster nodes and it is expected that the cloud traffic will be sent through eth0. For example, eth1 can be used for the cluster interconnect and eth0 for the cluster node IP, as illustrated in the graphic:

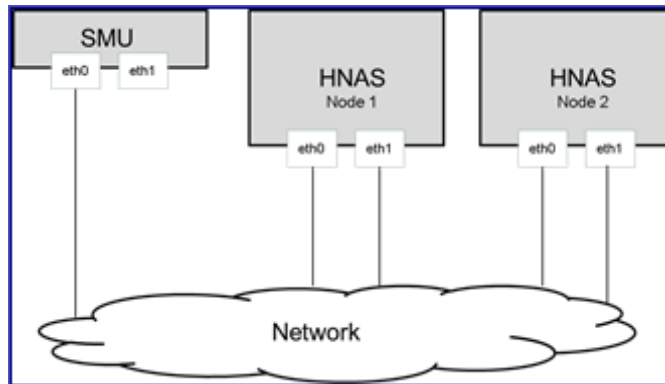


Hitachi Global Solutions and Services recommends the following network configuration for cloud traffic:

Single node network configuration:



Clustered network configuration



The first figure displays a single node network configuration and the second a clustered network configuration. Each node requires two IP addresses:

- One cluster node IP address on eth0 and eth1.
- One Admin EVS IP address on eth1.
 - This IP will failover between the nodes as needed so it is not important which node it is configured on.

The following tables show examples of an IP address configuration:

Single Node

Interface	IP
SMU eth0	172.10.10.11
Cluster Node IP eth0	172.10.10.13
Cluster Node IP eth1	172.10.10.14
Admin EVS IP eth0	172.10.10.15

Cluster

Interface	IP
SMU eth0	172.10.10.11
Cluster Node IP eth0	172.10.10.13
Cluster Node IP eth1	172.10.10.14
Admin EVS IP eth0	172.10.10.15
2 Cluster Node IP eth0	172.10.10.16
2 Cluster Node IP eth1	172.10.10.17



Note: The SMU does not require redundant network connectivity.

All IPs configured on eth1 and eth0 of the HNAS node(s) should be on the same subnet.

To configure a cluster node IP addresses on a management port, issue the following commands on the CLI:

```
ipaddr [-r] [-p <port>] [-I <addr> -m <mask>] [-c | --confirm]
```

For example, to add the address 192.168.53.116 to eth1 with netmask 255.255.248.0, issue the following CLI command:

```
ipaddr -p eth1 -I 192.168.43.116 -m 255.255.248.0
```

This requires DNS in order to resolve the cloud target. To configure DNS, the CLI `dnsserver` command can be used:

```
dnsserver add <server1> <server2>
```

For example the following command assigns DNS servers 192.168.45.10 and 192.168.45.11

```
dnsserver add 192.168.45.10 192.168.45.11
```

Make sure to configure a default route for the eth0 and eth1 interfaces. This can be done with the CLI `route` command:

```
route add gateway -g <addr>
```

For example the following command assigns default gateway 192.168.43.1.

```
route add gateway -g 192.168.43.1
```



Note: When the cloud target is HCP, Global Solutions and Services recommends the HCP and HNAS eth0 and eth1 interfaces reside on the same subnet.

These commands must be run once before configuring the cloud objects such as account and destination, and these settings are persistent across any reboot of the system. To modify or delete these settings, consult the man pages for the `ipaddr` and `route` commands.



Note: Using the `ipaddr` and `route` commands will not modify other addresses and routes already configured on the management interfaces.



Tip: To verify your routing and DNS configuration, the CLI `ping` and `host` commands can be used.

Data Migrator to Cloud Environment Variables

Data Migrator to Cloud provides two settings to control when migrated files are recalled from a cloud target. When using HCP as a cloud target, the files residing on HCP cannot be modified and can only be deleted. It is desirable to have the ability to modify migrated files. When enabled, the system will recall the file to the local file system when it is modified. The file can then be migrated back to HCP when the data migrator policy next runs and it meets the migration criteria defined in the data migrator policy.

Currently the system may not be able to recall all files that are being modified; this may result in an error. This is application dependent. Applications known to work are Microsoft Office applications. To provide better support for recall on write, the system has another variable, `xv1-auto-recall-on-read`, and when enabled, this setting will recall all files when read. Because the file will already reside locally on the system, all modifications will occur successfully.



Note: These variables are global cluster-wide settings. Global Solutions and Services recommends that these variables are not enabled when existing non-cloud HCP configurations are in use with other file systems.



Important: When `xv1-auto-recall-on-read` is enabled, replications will recall all migrated files.

To enable recall on write, set the environment variable `xv1-auto-recall-on-modify` through the CLI to true.

For example:

```
set xv1-auto-recall-on-modify true
```

To enable recall on read, set the environment variable `xv1-auto-recall-on-read` through the CLI to true.

For example:

```
set xv1-auto-recall-on-read true
```

Both of these variables take effect immediately.

Hitachi Vantara



Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact