IBM Spectrum Protect v. 8.1 on Hitachi NAS Platform 4060 Using the Network Data Management Protocol

Lab Validation Report

By Roman Friedman

October 2017
Feedback

Hitachi Vantara welcomes your feedback. Please share your thoughts by sending an email message to SolutionLab@hitachivantara.com. To assist the routing of this message, use the paper number in the subject and the title of this white paper in the text.

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SL-010-00</td>
<td>Initial release</td>
<td>October 31, 2017</td>
</tr>
</tbody>
</table>
# Table of Contents

**Product Features**  
Hitachi NAS Platform  
IBM Spectrum Protect  

**Test Environment Configuration**  
Network Configuration  
IBM Spectrum Protect Server Configuration  
Logical Configuration  
NDMP Configuration for Hitachi NAS Platform  
IBM Tape Library Configuration  
IBM Spectrum Protect Version 8.1 Server Configuration  
Label Tapes  

**Test Methodology**  
Scope  
General Testing Steps  
Test Scenario  

**References**  
Hitachi Vantara  
IBM
IBM Spectrum Protect v. 8.1 on Hitachi NAS Platform 4060
Using the Network Data Management Protocol

Lab Validation Report

Read the lab validation results for IBM® Spectrum Protect™ version 8.1 with Hitachi NAS Platform (HNAS) 4060 using firmware version 13.1 with the network data management protocol (NDMP). Backing up NAS storage over NDMP uses automated snapshot management, fully capturing all security descriptors. Depending on the type of NDMP backup used, the data may be diverted directly to tape drives from network attached storage attached by Fibre Channel, rather than going over the LAN.

Hitachi NAS Platform backup may protected data in a variety of ways, including the following:

- File system snapshots
- Local and remote object-based replication
- Local and remote file-based replication
- Synchronous disaster recovery for Hitachi NAS Platform

Often, the best solution includes one or more of these in addition to traditional backup.

Traditional backup uses an application, such as IBM Spectrum Protect, to schedule copies from primary storage to secondary storage.

The secondary storage may be one of the following:

- Disk attached to a Spectrum Protect media server
- Tape attached to a Spectrum Protect server
- Tape devices directly attached or SAN attached to Hitachi NAS Platform.

Regardless, Storage Protect server controls that target.

The NDMP protocol uses a server and client model.

- The Hitachi NAS Platform is the NDMP server (datamover)
- The Spectrum Protect server is the NDMP client, also called a data management application (DMA)

There are three NDMP backup models:

- Local NDMP
- Remote NDMP
- Three-way NDMP

**Note** — Support for NDMP is only offered in IBM Spectrum Protect extended version.
Performed tests were to ensure compatibility of the software and hardware components under specified conditions. The validation consisted of system-level tests emphasizing data movement through the NDMP device service for Hitachi NAS Platform. Testing is not intended to validate the functional capability of the IBM Spectrum Protect product nor Hitachi NAS Platform.

**Note** — Testing of this configuration was in a lab environment. Many things affect production environments beyond prediction or duplication in a lab environment. Follow the recommended practice of conducting proof-of-concept testing for acceptable results in a non-production, isolated test environment that otherwise matches your production environment before your production implementation of this solution.

### Product Features

These are the components used when testing this solution.

<table>
<thead>
<tr>
<th>TABLE 1. HARDWARE COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>Hitachi NAS Platform 4060</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Hitachi Unified Storage 130</td>
</tr>
<tr>
<td>Rack Optimized Server for Solutions, 2U Single Node</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IBM System Storage® T3200 Tape Library</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Brocade 6510 Switch</td>
</tr>
</tbody>
</table>
Hitachi NAS Platform

Hitachi NAS Platform is advanced and integrated network attached storage (NAS) solution. It provides a powerful tool for file sharing, file server consolidation, data protection, and business-critical NAS workloads.

- Powerful hardware-accelerated file system with multi-protocol file services, dynamic provisioning, intelligent tiering, virtualization, and cloud infrastructure
- Seamless integration with Hitachi SAN storage, Hitachi Command Suite, and Hitachi Data Discovery Suite for advanced search and index
- Integration with Hitachi Content Platform for active archiving, regulatory compliance, and large object storage for cloud infrastructure

Firmware version 13.1 in NAS Platform supports SMB3 encryption. This is currently a command line-only configuration. SMB3 data encryption protects against potential eavesdropping attacks on untrusted networks.

There is FMD-based compression support for Hitachi Virtual Storage Platform F series (VSP F series).

The server protects the health of the dynamic provisioning pool by preventing file system auto-expansion, returning any vacated chunks to the dynamic provisioning pool when physical space is depleted. Vacated chunks are regions of disk space that were formerly used by file systems that have since been deleted.

Local users and Microsoft® Active Directory® groups can now be created with SMU read-only access. A read-only user has permission to view most pages of the NAS Manager.

NAS platform supports data on an external server using Hitachi Universal Volume Manager (UVM).

In addition to existing VMware-based virtual SMU support, Microsoft Hyper-V® virtual SMU support is now provided for Microsoft Windows Server® users. This free option is available for download from the support portal.

The primary default deduplication database is the permabit database. However, NAS Platform now supports the Hitachi Protection Platform family deduplication database as a secure alternative.

IBM Spectrum Protect

IBM Spectrum Protect provides automated, centrally scheduled, policy-managed backup, archive, and space-management capabilities for file servers, workstations, virtual machines, and applications.

Reduce backup infrastructure costs by up to 53% with scalable high performance delivered entirely in software. Meet your price and performance objectives with a wide choice of cloud and on-premises storage options

Review the release notes for IBM Spectrum Protect server version 8.1.
Test Environment Configuration

When evaluating this solution, the tape library had been correctly attached previously to the Hitachi NAS Platform filer and the devices were configured for use. The basic IBM Spectrum Protect server configuration steps required to ready the environment for use are the following:

1. Define the Library.
2. Define the drives and their associated paths.
3. Define a device class for NDMP operations.
4. Define the storage pool for backups performed by using NDMP operations.
5. Optional: Select or define a storage pool for storing tables of contents for the backups.
6. Configure IBM Spectrum Protect Server policy for NDMP operations.
7. Register the Hitachi NAS Platform node with the server.
9. Label and check in media to the library

Network Configuration

Ethernet connectivity utilizing TCP/IP provided the communication path between the following:

- IBM Spectrum Protect management server and client (1 GbE network)
- IBM Spectrum Protect server and IBM TS3200 tape library (1GbE network)
- Hitachi Unified Storage 130 and Hitachi NAS Platform 4060 (10 GbE network)

IBM Spectrum Protect Server Configuration

The server used for testing was configured with the following hardware and software components:

- Rack optimized server for solutions, 2U single node
- Microsoft Windows Server 2016, standard edition
- IBM Spectrum Protect extended edition, version 8.1
- IBM Spectrum Protect operations center, version 8.1
- IBM Spectrum Protect backup-archive client for Microsoft Windows 8.1

Logical Configuration

Figure 1 on page 5 is the logical configuration of the test environment.
Figure 1

IBM Spectrum Protect Server

IBM Spectrum Protect Client

HNAS 4060

HUS 130

Brocade 6510

IBM TS3200

10 Gigabit Ethernet

8GB/s Fibre Channel

1 Gigabit Ethernet
NDMP Configuration for Hitachi NAS Platform

Hitachi NAS Platform and IBM Spectrum Protect use the NDMP protocol to execute requests, provide services, and move data. Each NAS Platform has its own NDMP-secured device file. The device file can be backed up and restored only by using NDMP.

Configure NAS Platform as described in the following:

- “NDMP Communications Setting for Hitachi NAS Platform ” on page 6
- “Options for Hitachi NAS Platform” on page 7
- “Snapshot Configuration for NDMP Backups on Hitachi NAS Platform” on page 7
- “NDMP Device Configuration on Hitachi NAS Platform” on page 8
- “DMP Device List for Hitachi NAS Platform” on page 10
- “Hitachi NAS Platform Device Access Details” on page 10

NDMP Communications Setting for Hitachi NAS Platform

The standard Hitachi NAS Platform configuration for NDMP is to use port 10000 for communications. This port value was used when configuring the 'DATAMOVER' within IBM Spectrum Protect. The user name and password (ndmp) was also used in the IBM Spectrum Protect configuration process. Figure 2 shows the NDMP settings used for NAS Platform.

When doing this in your environment, if the NDMP server is stopped, start it. Then, verify that the option to enable the NDMP server at boot is selected.

Figure 2
Options for Hitachi NAS Platform

These NDMP options for Hitachi NAS Platform were set to allow NDMP to work more efficiently. In your environment, failure to set these options may result in failed backup and restore operations.

To set the NDMP options utilizing SSH, connect to the system management unit (SMU) IP address for NAS Platform, and then select the NAS Platform that you want to set. Using the command line interface in NAS Platform, execute the following commands:

```
HNAS01:$ ndmp-option tokens on
HNAS01:$ ndmp-option report_as_fs_all
HNAS01:$ ndmp-option mover_window_adjust_recovery
```

Figure 3

```
SCISV-HNAS1-C-2:$ ndmp-option tokens on
SCISV-HNAS1-C-2:$ ndmp-option report_as_fs_all
SCISV-HNAS1-C-2:$ ndmp-option mover_window_adjust_recovery
```

Snapshot Configuration for NDMP Backups on Hitachi NAS Platform

It is best practice to back up from snapshots rather than a live file system. This ensures that the data is in a consistent state and will not be affected by ongoing file activity. Using snapshots also facilitates incremental backups.

From the Home page of the Web Manager, open **Data Protection** and then **NDMP History & Snapshots**. See Figure 4 on page 8.

- Click the **Automatically create snapshots** option and the **Delete snapshot when obsolete** option.
- Under **Automated Snapshot Retention**, set the period long enough to allow any differential backup to complete before the snapshot for the previous full backup to expire.

You may view and configure these settings with the `ndmp-snapshot-options` command from the Hitachi NAS Platform command line interface.
NDMP History & Snapshots

NDMP Backup History
- Clear NDMP backup records on all EVSs.
  - Note: These settings apply to tape backups and ADC, but not file replication.
  - Changes will result in a full backup, not an incremental one.

Snapshot Options

Automated Snapshot Use
- Do not automatically create snapshots, but backup from the live file system.
- Automatically create snapshots. (This option does not affect file replication snapshot usage.)

Automated Snapshot Deletion
- Delete snapshot after use
- Delete snapshot after next backup
- Delete snapshot when obsolete

Automated Snapshot Retention
- Set Retention Maximum To: 14 Days
- Note: This setting will affect file replication

NDMP Device Configuration on Hitachi NAS Platform

If you are configuring Hitachi NAS Platform, skip this procedure when exclusively using remote NDMP. In that case, the backup targets are on the IBM Spectrum Protect server.

Figure 5

EVS Details NW91

- Name: NW91
- EVS ID: 1
- Status: Online
- Type: File Services
- Enabled: Yes
- Preferred Cluster Node: SCISV-HNAS1-C-1
- EVS Security: Individual
- Default File System Security Mode: Unix (supports Windows)

File Systems
- EMC_NW_FileSystem1
- TSM81_FS
The Fibre Channel ports on Hitachi NAS Platform must be zoned with the tape drive ports in order for NAS Platform to assign pathing to the library's robotics and tape drives. Create zoning such that NAS Platform has visibility to the following:

- Tape drives
- Media changer
- NAS Platform Fibre Channel initiator ports

Any Fibre Channel initiator port on NAS Platform may be used. NAS Platform may access disk and tape targets over the same ports.

**Note** — Hitachi NAS Platform servers may share tape devices with other servers. However, always ensure SAN zoning does not allow other servers access to initiator ports or array controller ports used by Hitachi NAS Platform servers.

The IBM Spectrum Protect server executes requests, sending SCSI commands to NAS Platform using the NDMP protocol; which in turn passes these commands on to the tape library.

Special device files defined by Hitachi NAS Platform are used when configuring IBM Spectrum Protect. Use the file pathing information to define the specific paths by which IBM Spectrum Protect may access the tape library for which Hitachi NAS Platform is proxying. These files define both the tape library's robotic and drives. Without the device files association, successful backup and restore operations would not be possible.

Figure 7 and Figure 8 on page 10 show the configuration details for the Hitachi NAS Platform 4060 EVS used for testing.

Figure 7
DMP Device List for Hitachi NAS Platform

Ensure the targets have been discovered and are presented on the device list. There are two ways to display the device list.

- Using the Web Manager User Interface, from the **Home** page, click **Data Protection**, and then click **NDMP Device List**.
- Using the command line interface, type this command: `ndmp-devices-list`

The devices pathing used when testing this environment are the following:

- `/dev/mc_d5l1` (IBM TS3200 robotic control)
- `/dev/mt_d5l0` (Tape Drive 1)
- `/dev/mt_d6l0` (Tape Drive 2)
- `/dev/mt_d7l0` (Tape Drive 3)
- `/dev/mt_d6l0` (Tape Drive 4)

The NDMP device file information obtained from Hitachi NAS Platform is shown in Table 2.

**TABLE 2. NDMP DEVICE FILE INFORMATION FROM HITACHI NAS PLATFORM**

<table>
<thead>
<tr>
<th>EVS: Device Name</th>
<th>WWN Node (LUN)</th>
<th>Model</th>
<th>Serial Number</th>
<th>Allow Access</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NW91:/dev/mt_d8l0</td>
<td>20:01:00:0e:11:15:ba:2f(0)</td>
<td>IBM (3573-TL)</td>
<td>90WT066643</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NW91:/dev/mc_d5l1</td>
<td>20:01:00:0e:11:15:ba:2f(1)</td>
<td>IBM (ULT3580-HH6)</td>
<td>00L4U78W5978_LL0</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NW91:/dev/mt_d6l0</td>
<td>20:0a:00:0e:11:15:ba:2f(0)</td>
<td>IBM (ULT3580-HH6)</td>
<td>10WT046622</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NW91:/dev/mt_d7l0</td>
<td>20:04:00:0e:11:15:ba:2f(0)</td>
<td>IBM (ULT3580-HH6)</td>
<td>10WT046658</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NW91:/dev/mt_d8l0</td>
<td>20:07:00:0e:11:15:ba:2f(0)</td>
<td>IBM (ULT3580-HH6)</td>
<td>10WT046648</td>
<td>Allowed</td>
<td>OK</td>
</tr>
</tbody>
</table>

Hitachi NAS Platform Device Access Details

Each device must be granted access to an EVS. Granting access by an EVS to a device may be accomplished in one of two ways:

- Select the check box next to the devices.
- Click **Allow access** to grant access to the drives from every EVS, which is the Hitachi NAS Platform default.
The Hitachi NAS Platform server detects the devices automatically. If the devices are not displayed, do one of the following:

- Click the **Refresh Status** link.
- Run the **ndmp-devices-update** command from a command prompt.

Click the details link for each device and select each EVS that will use the device. If more than one EVS will use the device, from the **EVS** list, click **Any EVS**. Then, click **reassign**. From a command prompt, the **backup-device-set-evs** command may be used also to set this option.

In Figure 9 through Figure 13, shows the ALL EVS, including NW91 has been granted access to all tape drives and the tape robot.

- Figure 9 on page 11 shows robotic control access (/dev/mc_d5l1).
- Figure 10 on page 11 shows tape drive 1 access (/dev/mt_d5l0).
- Figure 11 on page 12 shows tape drive 2 access (/dev/mt_d6l0).
- Figure 12 on page 12 shows tape drive 3 access (/dev/mt_d7l0).
- Figure 13 on page 12 shows tape drive 4 access (/dev/mt_d8l0).

**Figure 9**

![Figure 9](image1)

**Figure 10**

![Figure 10](image2)
Allow the devices for NDMP use by one of the following:

- Click **allow access**.
- Run this command from a command prompt:
  ```
  backup-device-allow-access
  ```

Backup administrators may find it helpful in this situation to assign aliases to the tape drives that are easier to remember than the server’s device name or the tape drive’s serial number. Aliases may be assigned using one of the following:

- The user interface of Hitachi NAS Platform GUI
- From a command prompt, type this: `ndmp-device-assigned-name-set`
Figure 14 is output of configured tape devices on Hitachi NAS Platform.

**Figure 14**

```
SCISV-HNAS1-C-1:$ cn all scsi-tapes -a
Cluster node 1:
  Dev ID LUN Type Make Model Rev Capacity In Use Status Port
  17 0 tape IBM ULT3580-HH6 G9P1 n/a OK 5 online
  19 0 tape IBM ULT3580-HH6 G9P1 n/a OK 4 online
  20 0 tape IBM ULT3580-HH6 G9P1 n/a OK 3 online
  21 0 tape IBM ULT3580-HH6 G9P1 n/a OK 2 online
  18 1 robot IBM 3573-TL E.20 n/a OK 5 online
Cluster node 2:
  Dev ID LUN Type Make Model Rev Capacity In Use Status Port
  17 0 tape IBM ULT3580-HH6 G9P1 n/a OK 1 online
  19 0 tape IBM ULT3580-HH6 G9P1 n/a OK 3 online
  20 0 tape IBM ULT3580-HH6 G9P1 n/a OK 0 online
  21 0 tape IBM ULT3580-HH6 G9P1 n/a OK 2 online
  18 1 robot IBM 3573-TL E.20 n/a OK 1 online
```

Figure 15 shows the results from this NDMP command: `ndmp-option -I`

**Figure 15**

```
SCISV-HNAS1-C-1:$ ndmp-option -I
NDMP version offered(version): 4
NDMP port used(port): 10000
NDMP volume level quota backup(vqlb): on
NDMP volume level quota restore(vqlr): off
NDMP Backup performance stats(perf): record
NDMP obey hard quota limits(quotalimit): default
Block NDMP client access from these IP addresses(blockip): unset
Allow NDMP client access only from these IP addresses(allowip): unset
Enable use of token based incremental backups(tokens): on
2nd level read Ahead issuable by each lsv level read Ahead(ext_readAhead): 1 (0x1)
Maximum number of read Ahead processes used(readAhead_procs): 5 (0x5)
Use of changed object list for incremental backup/copy(change_list_incr): off
Use slave session instead of merely changing EVS context(disable_evs_override): off
Delete additional files copied by failed replication(tidy_failed_replic): off
Devices to be reserved using SCSI Reserve command(reserve_devices): all
Objects to be reported as File Systems for back up(report_as_fs): all
Minimum size of packet to send in bytes(min_send_size): 1024 (0x400)
Mover window adjustments applied to(mover_window_adjust): recovery
Block level replication override(Block_override): none
Ignore external links in NDMP backup operations unless the operation explicit requests
Port range for NDMP data connections(data port range): any
```

**Note** — Pay attention to the option shown in Figure 16 on page 13. This matters when using EMC Networker or Veritas NetBackup software.

**Figure 16**

```
reserve_devices [{ none | tape | autochanger | all]}
Enable use of SCSI reserve command to gain exclusive access to a device. The default is "none" meaning that the reserve command is not used. We recommend that this default is used unless you are trying to do tape device sharing with certain backup applications (such as Networker or NetBackup). If you enable reservation of a device then you should also select a preferred FC port to use to access that device. This can be achieved using the backup-device-port command. We recommend discussing this with your support provider before you make this change.
```
Figure 17 shows the details on CIFS share used for testing backups and restores.

### IBM Tape Library Configuration

Tape drives and robotics within a library must be defined to the IBM Spectrum Protect server. The tape drive position within the library must be specified as well.

Each tape drive location has a corresponding **element address**, defining its location. Many tape libraries specify the element address for each tape drive in the user interface, which is the case for IBM tape libraries. If element information is not readily available, consult the library manufacturer's user guide.

IBM also provides this web reference:


This is an example **IBM TS3200 (3573-TL)** configuration consisting of the following components:

- Four Fibre Channel-attached ULT3580-HH6 (LTO6) tape drives
- One robotic changer accessible via Tape Drive1
The **Element Address** for each drive is used to configure IBM Spectrum Protect server. The information in Figure 18 and Figure 19 on page 16 was obtained by accessing the library’s management graphical user interface, Monitor Library, and Drive Identity.

**Figure 18**

**TS3200 Tape Library**

<table>
<thead>
<tr>
<th>Library Identity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>78W3978</td>
</tr>
<tr>
<td>Product ID</td>
<td>3573-TL</td>
</tr>
<tr>
<td>Currently Installed Library Firmware</td>
<td>C.20 / 3.20e</td>
</tr>
<tr>
<td>Bootcode Firmware Revision</td>
<td>0.80</td>
</tr>
<tr>
<td>Barcode Reader</td>
<td>5E525</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>172.17.29.241</td>
</tr>
<tr>
<td>MAC Address</td>
<td>000E1115BA2F</td>
</tr>
<tr>
<td>Library Mode</td>
<td>Random</td>
</tr>
<tr>
<td>WWId Node Name</td>
<td>20000000E1115BA2F</td>
</tr>
</tbody>
</table>
### Figure 19

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>1 (LUN)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>90V7066643</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>GSP1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>255</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>20010000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Port Name</strong></td>
<td>20020000E1115BA2F</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>N-Port</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Automatic</td>
</tr>
<tr>
<td><strong>Port B</strong></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>10V7046649</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>GSP1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>255</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>20030000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Port Name</strong></td>
<td>20030000E1115BA2F</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>N-Port</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Automatic</td>
</tr>
<tr>
<td><strong>Port B</strong></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>10V7046649</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>GSP1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>255</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>20070000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Port Name</strong></td>
<td>20080000E1115BA2F</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>N-Port</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Automatic</td>
</tr>
<tr>
<td><strong>Port B</strong></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>10V7046622</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>GSP1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>259</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>200A0000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Port Name</strong></td>
<td>200B0000E1115BA2F</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>N-Port</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Automatic</td>
</tr>
<tr>
<td><strong>Port B</strong></td>
<td>Disabled</td>
</tr>
</tbody>
</table>
IBM Spectrum Protect Version 8.1 Server Configuration

The software installation and configuration for this project was done based on IBM Spectrum Protect for Windows Version 8.1.0 Installation Guide and covered in a separated HDS ISV team's document with identical title.

IBM Spectrum Protect 8.1 Administrator's solution guides for Windows may be downloaded from the following location:


Configure a Policy

To configure a policy, do the following.

1. Define a domain to be used for the Hitachi NAS Platform backups:

   Use this command: `define domain DOMAIN_NAME description="description"

   SERVER1>define domain HNASDOMAIN description='Policy Domain for HNAS'

   Figure 20

2. Define a policy set for the Hitachi NAS Platform domain.

   Use this command: `define policyset DOMAIN_NAME POLICY_SET_NAME

   SERVER1>def policyset HNASDOMAIN HNASPOLICY standard

   Figure 21

3. Define a management class for the Hitachi NAS Platform domain and policy set.

   Use this command: `define mgmtclass DOMAIN_NAME POLICY_SET_NAME CLASS_NAME

   SERVER1> def mgmtclass HNASDOMAIN HNASPOLICY HNASMGMT standard
4. Assign the HNAS management class as the default.
   
   Use this command:  `assign defmgmtclass DOMAIN_NAME POLICY_SET_NAME CLASS_NAME`
   
   ```
   SERVER1> assign defmgmtclass HNASDOMAIN HNASPOLICY HNASMGMT
   ```

Configure Storage Pools, Copy Groups, and Policy Sets
To configure storage pools, copy groups, and policy sets, do the following.

1. Create the TOC storage pool.
   
   Use this command:  `define stgpool STORAGE_POOL_NAME devclass`
   
   ```
   SERVER1> define stgpool NDMPPOOL HNASCLASS maxscratch=10 dataformat=ndmpdump
   ```
   - If a TOC is being created, create a storage pool for the TOC.
     ```
     SERVER1> define stgpool TOCPOOL DISK
     ```

2. Define the volume or volumes for of the TOC storage pool.
   
   Use this command:  `define volume TOC_POOL_NAME "TOC_POOL_LOCATION" access=type formatsize=SIZE_IN_MB`
   
   ```
   SERVER1> define volume tocpool "c:\tocpool\hnas_toc_vol1.dsm" access=readwrite formatsize=10000
   ```

3. Configure the management class to use the NDMP storage pool and write the catalog to the TOC storage pool.
   
   Define a copy group using this command:  `define copygroup DOMAIN_NAME POLICY_SET_NAME CLASS_NAME type=backup desitnation=NDMP_POOL_NAME tocdestination=TOC_POOL_NAME versexitst=# _versions`
   
   ```
   SERVER1> define copygroup HNASDOMAIN standard HNASMGMT destination=NDMPPOOL tocdestination=TOCPOOL verexists=4
   ```

4. Activate the policy set.
   
   Use this command:  `activate policyset DOMAIN_NAME POLICY_SET_NAME`
   
   ```
   SERVER1> activate policyset HNASDOMAIN HNASPOLICY
   ```

Register an EVS as an IBM Storage Protect Node and Configure it as a Datamover

In IBM Spectrum Protect, a node is a server that hosts the data. For Hitachi NAS Platform this host is the EVS. The Spectrum Protect client node and the EVS are synonymous.

To register an EVS as an IBM Storage Protect node and configure it as a datamover, do the following.

1. Register the node with this type:  `NAS`
   
   Use this command:  `register node HOST_NAME password userid=user_id domain=DOMAIN_NAME type=NAS`
   
   ```
   SERVER1> register node MW91 password1 userid=EVSNW91 domain=HNASDOMSAIN type=NAS
   ```
2. Define a datamover to the IBM Spectrum Protect server.

   Use these commands:

   define datamover HNAS_EVS type=NAS
   HLAddress=EVS_IPAddress
   LLAddress=tcpportofHNAS
   USERid=usernameforHNAS
   Password=passwordofHNAS
   Online=yes
   dataformat=NDMPDump

   SERVER1>define datamover MW91 type=NAS
   HLAddress=xxx.xxx.xxx.xxx
   LLAddress=10000
   userid=ndmp
   password=ndmp
   dataformat=ndmpdump
   online=yes

   **Note** — LLAddress, userid, and password are obtained from Hitachi NAS Platform communications settings. See Figure 22

**Figure 22**

![Command Builder - SERVER1](image)

---

- SERVER1> query policyset
- Policy Domain Name | Policy Set Name | Default Mgmt Class Name | Description
- HNASADMIN | HNASPOLICY | HNASMGMT | policyset for domain
- STANDARD | ACTIVE | STANDARD | Installed default policy set.
- STANDARD | STANDARD | STANDARD | Installed default policy set.

- SERVER1> register node NW91 password
- ANR2060I Node NW91 registered in policy domain STANDARD.

- SERVER1> register node NW91 password userid=nw91 domain=HNASDOMAIN type=nas
- ANR2147E REGISTER NODE: Node NW91 is already registered.
- Return code 10.

- SERVER1> remove node NW91
- Do you want to proceed? (Yes/No) [N] y
- ANR2061I Node NW91 removed from policy domain STANDARD.

- SERVER1> define datamover MW91 type=NAS
- HLaddress=172.17.38.127
- userid=ndmp
- password=ndmp
- dataformat=ndmpdump
- online=yes
- ANR1730I Data mover MW91 has been defined.
Define Tape Library, Tape Drives, and Path to Drives

To define the tape library, tape drives, and the path to drives, do the following.

1. Define the library to the IBM Spectrum Protect server.
   
   Use this command: `define library HNASlib libtype=scsi libtype=SCSI`

   ```
   SERVER1> define library HNASlib libtype=scsi
   ```

2. Define a path to the library (Figure 23).
   
   Use this command: `define path datamover (EVS_NAME) LIBRARY_NAME desttype=library device=CHANGER_SPECIAL_FILE_NAME online=y/n`

   ```
   SERVER1> define path MW91 HNASLIB srctype=datamover desttype=library device=/dev/mc_d5l1 online=yes
   ```

Figure 23
3. Define the drives that are attached to the library (Figure 25).

Use this command: `define drive DRIVE_NAME element=ELEMENT_NUMBER online`

SERVER1>define drive HNASLIB TAP01 element=256
SERVER1>define drive HNASLIB TAP02 element=257
SERVER1>define drive HNASLIB TAP03 element=258
SERVER1>define drive HNASLIB TAP04 element=259

**Note** — Before proceeding to define paths to drives, pay attention to the serial number and element address for each drive, as shown in Figure 24 on page 22.
### Figure 24

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>1 (LUN)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>90WT066643</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>G39P1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>256</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>2001000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Port Name</strong></td>
<td>2002000E1115BA2F</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>N-Port</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Automatic</td>
</tr>
<tr>
<td><strong>Port B</strong></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>10WT046658</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>G39P1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>257</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>2004000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Port Name</strong></td>
<td>2005000E1115BA2F</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>N-Port</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Automatic</td>
</tr>
<tr>
<td><strong>Port B</strong></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>10WT046648</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>G39P1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>255</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>2007000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Port Name</strong></td>
<td>2008000E1115BA2F</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>N-Port</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Automatic</td>
</tr>
<tr>
<td><strong>Port B</strong></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drive Identity</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor ID</strong></td>
<td>IBM</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>ULT3580-HH6</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>10WT046622</td>
</tr>
<tr>
<td><strong>Firmware Revision</strong></td>
<td>G39P1</td>
</tr>
<tr>
<td><strong>Element Address</strong></td>
<td>259</td>
</tr>
<tr>
<td><strong>Control Path Drive</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Data Compression</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Fibre Channel</td>
</tr>
<tr>
<td><strong>Node Name</strong></td>
<td>2004000E1115BA2F</td>
</tr>
<tr>
<td><strong>Port A</strong></td>
<td>Enabled</td>
</tr>
</tbody>
</table>
4. Associate each tape drive and each defined element with the serial number of the NDMP devices and appropriate device names in Hitachi NAS Platform (Figure 25).

**Figure 25**

<table>
<thead>
<tr>
<th>*EVS/Device Name</th>
<th>WWN Node (LUN)</th>
<th>Manufacturer (Model)</th>
<th>Serial Number</th>
<th>Allow Access</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUV51/devint_d600</td>
<td>20:01:00:0e:11:15:be:3f (1)</td>
<td>IBM (3573 TL)_</td>
<td>8064U78707878L_ID</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NUV51/devint_d600</td>
<td>20:31:00:0e:11:15:be:3f (6)</td>
<td>IBM (UL3580-961)</td>
<td>90V7840543</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NUV51/devint_d700</td>
<td>20:04:00:0e:11:15:be:3f (6)</td>
<td>IBM (UL3580-961)</td>
<td>90V78405322</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NUV51/devint_d700</td>
<td>20:04:00:0e:11:15:be:3f (6)</td>
<td>IBM (UL3580-961)</td>
<td>90V7840530</td>
<td>Allowed</td>
<td>OK</td>
</tr>
<tr>
<td>NUV51/devint_d800</td>
<td>20:07:00:0e:11:15:be:3f (6)</td>
<td>IBM (UL3580-961)</td>
<td>90V7840532</td>
<td>Allowed</td>
<td>OK</td>
</tr>
</tbody>
</table>

5. Define a path to the drives (Figure 26 on page 24).

Use this command: `define path datamover (EVS_NAME) Tape_Drive_Name srctype=datamover desttype=drive library=hnaslib device=/dev/ mc_xxxx`

SERVER1>define path MW91 TAP01 srctype=datamover desttype=drive library=HNASLIB device=/dev/ mt_d510
SERVER1>define path MW91 TAP02 srctype=datamover desttype=drive library=HNASLIB device=/dev/ mt_d610
SERVER1>define path MW91 TAP03 srctype=datamover desttype=drive library=HNASLIB device=/dev/ mt_d710
SERVER1>define path MW91 TAP04 srctype=datamover desttype=drive library=HNASLIB device=/dev/ mt_d810
Figure 26

38-111> q drive HNASLIB format=detailed
Library Name: HNASLIB
  Drive Name: TAP01
  Device Type: REMOTE
  On-Line: NO
  Read Formats:
  Write Formats:
    Element: 256
  Drive State: EMPTY
  Volume Name: 
  Allocated to: 
    WWN: 
  Last Update by (administrator): IBM-OC-38-111
  Last Update Date/Time: 2017-08-30, 20:38:00
Cleaning Frequency (Gigabytes/ASNEEDED/NONE): NONE

Library Name: HNASLIB
  Drive Name: TAP02
  Device Type: REMOTE
  On-Line: YES
  Read Formats:
  Write Formats:
    Element: 257
  Drive State: EMPTY
  Volume Name: 
  Allocated to: 
    WWN: 
  Last Update by (administrator): IBM-OC-38-111
  Last Update Date/Time: 2017-08-29, 14:18:34
Cleaning Frequency (Gigabytes/ASNEEDED/NONE): NONE

Library Name: HNASLIB
  Drive Name: TAP03
  Device Type: REMOTE
  On-Line: YES
  Read Formats:
  Write Formats:
    Element: 258
  Drive State: EMPTY
  Volume Name: 
  Allocated to: 
    WWN: 
  Last Update by (administrator): IBM-OC-38-111
  Last Update Date/Time: 2017-08-29, 14:18:55
Cleaning Frequency (Gigabytes/ASNEEDED/NONE): NONE

Library Name: HNASLIB
  Drive Name: TAP04
  Device Type: REMOTE
  On-Line: YES
  Read Formats:
  Write Formats:
    Element: 259
  Drive State: EMPTY
  Volume Name: 
  Allocated to: 
    WWN: 
  Last Update by (administrator): IBM-OC-38-111
  Last Update Date/Time: 2017-08-29, 14:19:10
Cleaning Frequency (Gigabytes/ASNEEDED/NONE): NONE
6. Define device class for Hitachi NAS Platform.

Use these commands:

```
define devclass DEVICE_CLASS_NAME Devtype=NAS library=LIBRARY_NAME
mountretention= MOUNT_RETENTION_PERIOD estcapacity= CARTRIDGE_CAPACITY (GB)
```

```
SERVER1> define devclass HNASCLASS devtype=NAS library=HNASLIB
mountretention=0 estcapacity=1500g
```

Figure 27 and Figure 28 are the results of running these configuration commands on SERVER1 Command Builder.

**Figure 27**

![Command Builder - SERVER1](image1)

**Figure 28**

```
38-111> query datamover type=nas format=detailed
Data Mover Name  Data Mover Type  IP Address          TCP/IP Port Number
Nw91   NAS       172.17.38.127    10000    ndmp    NDMP Dump    Yes
```
Label Tapes

To label and check the tape volumes into the library, type this command.

```
SERVER1> label libvol HNASLIB search=yes labelsource=barcode checkin=scratch
```

**Figure 29**

```
SERVER1> label libvol HNASLIB search=bulk labelsource=barcode checkin=scratch
```

Use `search=bulk` if this is a new tape located in the I/O slot:

**Figure 30**

The way the IBM Spectrum Protect is designed, you need to run the `audit library` command often. Otherwise you could observe the messages seen in Figure 30 in IBM Spectrum Protect Operations Center.

**Figure 31**

Figure 31 is the dashboard view.
See confirmation of auditing volume ANR8459I in Figure 32

**Figure 32**

![Audit Library Command Output]

To have a total view of all configured volumes in the database, use this command: **q libvolume**

**Figure 33**

<table>
<thead>
<tr>
<th>Library</th>
<th>Name</th>
<th>Volume Name</th>
<th>Status</th>
<th>Owner</th>
<th>Last Use</th>
<th>Home Element</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>HNASLIB</td>
<td>A00007L6</td>
<td>Private</td>
<td>Data</td>
<td>4,137</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HNASLIB</td>
<td>A00010L6</td>
<td>Private</td>
<td>Data</td>
<td>4,106</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HNASLIB</td>
<td>A00012L6</td>
<td>Private</td>
<td>Data</td>
<td>4,105</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HNASLIB</td>
<td>A00016L6</td>
<td>Private</td>
<td>Data</td>
<td>4,129</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HNASLIB</td>
<td>A00035L6</td>
<td>Private</td>
<td>Data</td>
<td>4,099</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HNASLIB</td>
<td>A00038L6</td>
<td>Private</td>
<td>Data</td>
<td>4,110</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HNASLIB</td>
<td>A00039L6</td>
<td>Scratch</td>
<td></td>
<td>4,098</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Test Methodology**

This is an overview of the testing requirements to demonstrate interoperability of IBM Spectrum Protect software with Hitachi NAS Platform 4100 using network data management protocol (NDMP). These results may be applicable for other network attached storage devices.

**Scope**

Very extensive testing was done in 2014 by Hitachi for IBM TSM version 7.1 with the same version 12 firmware used on Hitachi NAS Platform 4060. Because of this previous testing, testing this time involved using a three times larger scoop of data and files, but minimized the number of backup tests to the following:

- Two full and two differential backups on the Hitachi NAS Platform CIFS share with TOC
- One additional Microsoft Windows Server 2016 node backup
- One NDMP CIFS share directory restoration that was intentionally deleted
**General Testing Steps**

Most of the testing procedures have a flow that is very similar. For backups and restores, the following steps were completed for testing:

1. The file system or share to be backed up was sized. The byte count, number of files, and directories was noted.
2. A backup or restore command was issued.
3. The *query process* command was issued a number of times during the process to confirm that the job is running, note its progress, the process number, and the tape volume mounted.
4. After the backup and restore jobs had completed, the Activity Log information was viewed to determine successful completion of the job.
5. A comparison was made of pre-backup and post-backup byte counts and files

**Test Scenario**

This is the test scenario used to validate the solution.

**Directory Listing of the File System**

Figure 34 shows the CIFS share test with its directories, which was backed up completely with full backup option.

**Figure 34**
Figure 35 shows the properties of one of subdirectories in the test share that was backed up.

**Figure 35**

![Qual_Data Properties](image)

**Type:** File folder  
**Location:** Y:\  
**Size:** 24.0 GB (25,805,394,277 bytes)  
**Size on disk:** 737 GB (792,385,814,528 bytes)  
**Contains:** 365,410 Files, 9 Folders  
**Created:** Wednesday, July 12, 2017, 12:40:55 PM  
**Attributes:**  
- Read-only (Only applies to files in folder)  
- Hidden  
- Archive

**Start Full Backup**

This command was used to start the backup.

```
SERVER1> TSM-NODE1> backup node MW91 /__VOLUME__/EMC_NM_FileSystem1 mgmtclass=HNASMGMT toc=yes mode=full type=backupimage
```

**Figure 36**

![Event Log](image)
Figure 37 shows the command line output from backing up over 51 GB of data.

Figure 37

AS platform volumes, file systems, and CIFS share have been used for backup and restore testing, as shown in Figure 38. The CIFS share test was populated with data, which included a directory consisting of over 10 million files of varying sizes. The same share’s subdirectory was used to restore a backup to an original location and verify that backup data matched the restore data.

To sample the TOC post-backup, these commands were typed:

```
SERVER1> q toc MW91 /__ VOLUME__/EMC_NW_FileSystem1 format=detailed
```

You can observe creation of a new snapshot, triggered by backup command in Command Builder.

Figure 38
IBM Spectrum Protect server also leaves logs and proof of a successful TOC backup within backup directory.
Directory Pre-Restore

Figure 42 shows the properties of the nqt_data director before restoration.

**Figure 42**
The nqt_data directory with 15,434 files and total size 4.25 GB is intentionally deleted (Figure 43).

**Figure 43**

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$<em>CFN</em></td>
<td>4/27/2017 5:16 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>$<em>NDMP</em></td>
<td>5/9/2017 4:41 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>nqt_data</td>
<td>5/9/2017 1:50 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>NW</td>
<td>5/2/2017 12:19 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>nw_nfs</td>
<td>5/2/2017 12:57 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Qual_Data</td>
<td>7/12/2017 12:41 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Qual_Data</td>
<td>10/20/2014 11:10 PM</td>
<td>Compressed (zipped) Folder</td>
<td>20,054,927 KB</td>
</tr>
</tbody>
</table>

Begin Restoration of Node MW91
The following command was issued to begin the restoration of node NW91.

```
SERVER1 > restore node MW91 /__VOLUME__/EMC_NW91_FileSystem1 pdate==today
```

Monitor Process in a Command Line Interface Window
The restoration process was monitored in a command line interface window.

Results of Full Restore From the Tape Volume A00039L6
Figure 44 shows a full restoration from the tape volume.
Deleted nqt_data Directory Restored

Figure 45 on page 34 and Figure 46 on page 35 show that the nqt_data directory was restored to its size before deletion.

**Figure 45**

![Filesystem view of nqt_data directory](image)
## Figure 46

<table>
<thead>
<tr>
<th>Source</th>
<th>Volume Serial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive 1 (1)</td>
<td>A00007L6</td>
</tr>
<tr>
<td>I/O Station 2</td>
<td>A00011L6</td>
</tr>
<tr>
<td>I/O Station 3</td>
<td>A00006L6</td>
</tr>
<tr>
<td>Slot 1 (1)</td>
<td>A00009L6</td>
</tr>
<tr>
<td>Slot 2 (1)</td>
<td>A00010L6</td>
</tr>
<tr>
<td>Slot 3 (1)</td>
<td>A00012L6</td>
</tr>
<tr>
<td>Slot 4 (1)</td>
<td>FL0147</td>
</tr>
<tr>
<td>Slot 5 (1)</td>
<td>380AABL5</td>
</tr>
<tr>
<td>Slot 9 (1)</td>
<td>A00008L6</td>
</tr>
<tr>
<td>Slot 12 (1)</td>
<td>A00019L6</td>
</tr>
<tr>
<td>Slot 15 (1)</td>
<td>A00014L6</td>
</tr>
<tr>
<td>Slot 16 (1)</td>
<td>A00015L6</td>
</tr>
<tr>
<td>Slot 17 (1)</td>
<td>A00016L6</td>
</tr>
<tr>
<td>Slot 18 (1)</td>
<td>A00017L6</td>
</tr>
<tr>
<td>Slot 19 (1)</td>
<td>A00018L6</td>
</tr>
<tr>
<td>Slot 45 (1)</td>
<td>CLNU50L1</td>
</tr>
</tbody>
</table>
Here is IBM Tape Library view with volume A00007L6 in Drive 1 performing restore operation.

**Figure 47**
As backup process continues, you can also observe the Event Viewer in the graphical user interface of the SMU for Hitachi NAS Platform (Figure 49 and Figure 50).
Hitachi NAS Platform created a new snapshot once IBM Spectrum Protect executed the CIFS share backup and removed the old snapshot after ending creating a new snapshot.

Figure 51

The results are in Figure 52.

Figure 52

Differential CIFS Share Backup

Figure 53 on page 38, Figure 54 on page 38, and Figure 55 on page 39 show a differential CIFS share backup.

Figure 53

Figure 54
Figure 55

Results of All Backup Jobs

Figure 56 shows the results of all backup jobs in the command line interface.

Figure 56
Figure 57 shows the results of backing up on IBM Spectrum Protect of the System State directory of the Microsoft Windows Server 2016 node.

**Figure 57**

![Backup Report](image)

**Note** — The network's transfer rate in Figure 57 is 107 MB/s.
Figure 58 shows the view in Operations Center for IBM Spectrum Protect of the client's backup.

**Figure 58**

---

**References**

These are references for this lab validation report.

**Hitachi Vantara**

This reference is available from the Knowledge website.

- [Backup Administration Guide: Hitachi Virtual Storage Platform Gx00 and VSP Fx00 with NAS Modules and Hitachi NAS Platform, Release 13.2](MK-92HNAS007-12, PDF)

**IBM**

These references are available from the IBM website.

- [Configuring Tivoli Storage Manager for NDMP operations](Tivoli® is an earlier name for Spectrum Protect)
- [IBM Spectrum Protect documentation]
For More Information

Hitachi Vantara Global Services offers experienced storage consultants, proven methodologies and a comprehensive services portfolio to assist you in implementing Hitachi products and solutions in your environment. For more information, see the Services website.

Live and recorded product demonstrations are available for many Hitachi products. To schedule a live demonstration, contact a sales representative. To view a recorded demonstration, see the Resources website.

Hitachi Vantara Academy provides best-in-class training on Hitachi products, technology, solutions and certifications. Hitachi Data Systems Academy delivers on-demand web-based training (WBT), classroom-based instructor-led training (ILT) and virtual instructor-led training (vILT) courses. For more information, see the Hitachi Data Systems Services Training and Certification website.

For more information about Hitachi products and services, contact your sales representative or channel partner or visit the Hitachi Vantara website.