Veritas NetBackup 7.0 Application Introduction

This document provides information needed to integrate a Data Domain system as a backup target for Veritas NetBackup (NBU) 7.0 storage software from Symantec.

This document covers the topics shown in the following table:

<table>
<thead>
<tr>
<th>Related Documents</th>
<th>Page 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Introduction</td>
<td>Page 5</td>
</tr>
<tr>
<td>Software Configuration</td>
<td>Page 9</td>
</tr>
<tr>
<td>Advanced Topics</td>
<td>Page 32</td>
</tr>
</tbody>
</table>

You can also go directly to the procedures indicated in the table below:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open the NBU Console</td>
<td>9</td>
</tr>
<tr>
<td>View Licenses</td>
<td>10</td>
</tr>
<tr>
<td>Configure DNS and AD Entries for the Data Domain System</td>
<td>13</td>
</tr>
<tr>
<td>Configure DFS Shares on a Windows NBU Media Server</td>
<td>13</td>
</tr>
<tr>
<td>Configure a BasicDisk STU</td>
<td>13</td>
</tr>
<tr>
<td>Configure a VTL STU</td>
<td>16</td>
</tr>
<tr>
<td>Verify NDMP Installation on the NBU Media Server</td>
<td>21</td>
</tr>
<tr>
<td>Configure an NDMP STU</td>
<td>21</td>
</tr>
<tr>
<td>Configure a Backup Policy</td>
<td>23</td>
</tr>
<tr>
<td>Manually Run a Back Up</td>
<td>24</td>
</tr>
<tr>
<td>Restore Backed Up Data</td>
<td>24</td>
</tr>
<tr>
<td>Configure Required NetBackup Global Settings</td>
<td>25</td>
</tr>
<tr>
<td>Configure Logging</td>
<td>29</td>
</tr>
<tr>
<td>View Unified Logs</td>
<td>29</td>
</tr>
<tr>
<td>Debug a NBU Failed Job (Example)</td>
<td>29</td>
</tr>
<tr>
<td>Resolve Failure After NBU 7.0 Upgrade on Windows</td>
<td>31</td>
</tr>
<tr>
<td>Set Up an SSO Configuration</td>
<td>32</td>
</tr>
<tr>
<td>Configure Replication and Restore from a Replica</td>
<td>37</td>
</tr>
</tbody>
</table>
Related Documents

Data Domain and Veritas NetBackup documents referred to in this guide provide additional information you need to integrate the backup software with the Data Domain system.

Access to Veritas NetBackup Documents

The following table lists the URLs for the referenced NBU documents.

<table>
<thead>
<tr>
<th>Title</th>
<th>URL</th>
</tr>
</thead>
</table>

Access to Data Domain Documents

The Documentation page at https://my.datadomain.com/documentation provides access to three categories of documents that are related to use of this application with Data Domain products:

- User guides referred to in this document, under Product Documentation.
- The latest version of this NetBackup Application Introduction along with other integration-related documents, under Integration Documentation.
- Compatibility matrices that show which components are compatible with each other, under Compatibility Matrices:
  - Data Domain hardware product numbers
  - Data Domain operating system (DD OS) versions
  - NBU server and client operating system versions
  - NBU software versions
  - Hardware driver versions
Product Introduction

Veritas NetBackup software from Symantec is a heterogeneous backup and recovery suite for large-scale enterprises. NBU provides backup, recovery, archive, retrieval, and disaster recovery with pools of storage units.

The four main types of NBU software installation options are described in the following table.

<table>
<thead>
<tr>
<th>Table 1: Four NBU Software Installation Types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software Type</strong></td>
</tr>
<tr>
<td>Master Server</td>
</tr>
<tr>
<td>Media Server</td>
</tr>
<tr>
<td>Client</td>
</tr>
<tr>
<td>Private Branch Exchange (PBX)</td>
</tr>
</tbody>
</table>

Product Installation

For how to install NBU software, refer to the NBU installation guide.

**Note:** When this document refers to any UNIX or UNIX-based operating system such as Linux, HP-UX, or Solaris, the term UNIX operating system is used.

Terms

The following Data Domain and NBU-specific terms are used in this document.

<table>
<thead>
<tr>
<th>Table 2: Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Term</strong></td>
</tr>
<tr>
<td>Data Domain system</td>
</tr>
<tr>
<td>High water mark (HWM)</td>
</tr>
<tr>
<td>Low water mark (LWM)</td>
</tr>
<tr>
<td>NetBackup Job</td>
</tr>
<tr>
<td>Policy</td>
</tr>
</tbody>
</table>
Differences Between File Device and VTL STUs

NBU can use a Data Domain system as a file device if the Data Domain System is configured with either the Basic Disk (NFS, CIFS) or OST STU configuration.

The differences between use of the Data Domain system as a file device or as a VTL STU are as follows:

- A File Device STU presents itself as disk destination storage.
- A VTL storage device emulates a physical tape library (PTL) and physical tape drives.

Table 3: Trade-offs Between VTL and File Device Configurations

<table>
<thead>
<tr>
<th>VTL</th>
<th>File Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A changer driver and tape driver that have been tested and posted as supported in the Data Domain compatibility matrix must be installed and loaded on the NBU media server</td>
<td>• No changer driver and tape driver installation and loading is required on the NBU media server</td>
</tr>
<tr>
<td>• A Fibre Channel HBA that has been tested and posted as supported in the Data Domain compatibility matrix must be installed on the NBU media server</td>
<td>• A Fibre Channel HBA is not required</td>
</tr>
<tr>
<td>• Because a VTL emulates a PTL, the backup software has to perform tape mounts, loads, labeling and other tape-emulation tasks even though there are no tapes.</td>
<td>• No tape mounts, loads, labeling or other tape emulation tasks are performed.</td>
</tr>
</tbody>
</table>
Restrictions and Limitations

This section describes restrictions and limitations when they affect NBU integration with Data Domain systems.

VTL Restrictions

When NBU is on a server that runs a version of the Windows operating system and when the Data Domain system is configured as a VTL STU, the following actions are likely to mark media changers and tape drives as down from the NBU perspective:

- Data Domain system reboot
- VTL restart
- Filesystem restart

To detect the possible removal of any devices, perform the following procedure after any of the above actions.

▼ Verify Discovery of Media Changers and Tape Devices

1. Go to Start > Settings > Control Panel > Administrative Tools > Computer Management > Device Manager. Verify that the media changers and tape devices are discovered.

2. If the devices have been deleted, perform the appropriate actions on the physical level and the operating system level and perform step 1 again.

3. Once the devices are discovered by the Windows device manager, use the NBU GUI to make sure they are enabled.

### Table 3: Trade-offs Between VTL and File Device Configurations

<table>
<thead>
<tr>
<th>VTL</th>
<th>File Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expired backup images are not cleaned up on the Data Domain system.</td>
<td>Expired backup images are cleaned up on the Data Domain system.</td>
</tr>
<tr>
<td>Pro – NetBackup can execute its tape import procedure to quickly recover and restore backup images.</td>
<td>Pro – Expired disk space is recycled immediately when garbage collection and cleaning kicks off.</td>
</tr>
<tr>
<td>Con – Expired disk space cannot be recycled immediately when garbage collection and cleaning kicks off.</td>
<td>Con – NBU is not able to recover and restore backup images as quickly.</td>
</tr>
<tr>
<td>Replication is easier. There is no need to configure CIFS access or NFS access to the STU.</td>
<td>CIFS or NFS mounts of the Data Domain system must be configured with the proper mount options on the NBU media server.</td>
</tr>
</tbody>
</table>
**Filesystem Restrictions**

The restrictions in the following table apply when the Data Domain system is configured as a file device.

**Table 4: Filesystem Restrictions**

<table>
<thead>
<tr>
<th>Restriction</th>
<th>NFS</th>
<th>CIFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always use either the nolock or llock mount option (depending on the operating system version). These options are required because by default NBU 7.0 media servers try to lock the files but fail; locking of files via NFS is not supported on a Data Domain system. Specify a 10 GB or smaller fragment size for the disk storage unit (DSU) when using Data Domain replication.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note:** Refer to the *Data Domain DD OS 4.x Quick Start Guide* and to the documentation for the NBU media server's operating system for other recommended mount options.

**Microsoft Cluster with Data Domain VTL Restrictions**

The following restrictions apply when a Data Domain system is configured as a VTL STU with Microsoft Cluster nodes:

- Both Microsoft Cluster nodes (initiators) connected to the Data Domain VTL must have HBAs from the same HBA vendor. This avoids issues with device port mapping of the changer that occur if different HBA vendors are used in the cluster nodes.
- Both cluster nodes must run version 4.4.2.x.x or a higher release.
- The IBM LTO driver must be at version 6.1.8.0 or higher for use with the 64-bit version of Windows.
Software Configuration

You can use the wizards in the NetBackup Administration Console to configure storage and policies. Figure 1 shows the NetBackup Administration Console with the configuration wizards in the right pane.

**Note:** All NBU GUI examples are from NetBackup 7.0.

**Note:** In command examples when you can enter a path in either a UNIX or Windows operating system, -> is shown as a path separator, instead of either (\) or (/). For example, if an example shows install--->bin, you would type install/bin (UNIX) or install\bin (Windows).

**Note:** In this document, the NetBackup Administration Console is referred to as the NBU console.

![NetBackup Administration Console](image)

**Figure 1:** NBU Console

▼ **Open the NBU Console**

The two following procedures describe how to open the NBU console.

▼ **Open the NBU Console on a UNIX Operating System**

1. Log in as a user authorized to run NetBackup to an NBU master or media server that runs a UNIX operating system.
2. Enter `/opt/openv/netbackup/bin/jnbSA&` on the command line.

```
# /opt/openv/netbackup/bin/jnbSA&
```

▼ Open the NBU Console on a Windows Operating System

1. Log into the Windows server as a user authorized to run NetBackup.
2. Select Start > All Programs > Veritas Netbackup > NetBackup Administration Console.

![Open an NBU Console on a Windows Operating System](image.png)

**Figure 2:** Open an NBU Console on a Windows Operating System

▼ View Licenses

On the Data Domain system and on NetBackup, advanced features and most add-ons require additional licenses. For example, NetBackup’s Shared Storage Option (SSO), is a licensed feature, and replication is a licensed feature in the Data Domain system.

The two following procedures describe how to view the needed licenses.

▼ View Data Domain System Installed Licenses

1. Connect to a Data Domain Enterprise Manager Web console.
2. Select Licenses.

**Figure 3** shows an example of feature licenses installed on a Data Domain system.
Review NetBackup Installed Licenses

1. Run `get_license_key` from the `NetBackup_install_path→netbackup→bin→admincmd` directory.

2. Click Help on the NetBackup Administration Console and select License Keys to view the installed licenses.

   Figure 4 shows an example of installed licenses displayed on a Windows server.
BasicDisk STU Configuration

A Data Domain system can be configured as a BasicDisk STU when it is either NFS—or CIFS—mounted on an NBU media server.

On a NBU media server that runs a version of the Windows operating system, you can specify the absolute pathname to directory to access the Data Domain system with either the Universal Naming Convention (UNC) or the DFS path name.

NFS Guidelines

The example in Figure 5 shows a NFS mount of a Data Domain system volume on a non-production UNIX system. Refer to the *Data Domain DD OS 4.x Quick Start Guide* for recommended mount options.

---

**Figure 4:** Installed Licenses on a Windows Server

**Figure 5:** NFS-mounted Volume on a Non-production UNIX System
CIFS Guidelines in a Windows AD Environment

In an Active Directory (AD) environment, the NBU server may fail to connect to a Data Domain system with the default system account if DNS and AD parameters are not set up correctly. Make sure all the needed set up is performed, as described in “Configure DNS and AD Entries for the Data Domain System.”

Also in an AD environment, Distributed File System (DFS) pathnames provide more-convenient access to Data Domain system targets for disaster recovery. When you configure a CIFS Basic Disk STU on a NBU media server in a Windows AD environment, use the DFS path name to specify the path to a Data Domain system as described in “Configure DFS Shares on a Windows NBU Media Server” on page 13.

▼ Configure DNS and AD Entries for the Data Domain System

1. On the Data Domain system, perform these steps:
   a. Configure the domain name.
   b. Configure the Data Domain system hostname using the fully qualified name.
   c. Configure an entry for the DNS server.

2. On the DNS server, make sure that DNS host entries are set up for the Data Domain system for both forward and reverse lookups.

3. Verify that an entry for the Data Domain system exists with the correct fully qualified name in the AD tree.

▼ Configure DFS Shares on a Windows NBU Media Server

Perform the following configuration steps to set up a Data Domain system with DFS shares on an NBU media server that runs Windows.

1. Create an active/passive setup for the distributed filesystem target for DR, restore or vaulting from the secondary Data Domain system. Make sure the secondary Data Domain system does not have a mapped DFS share that is active.

2. When the secondary Data Domain system is ready to be used for disaster recovery (DR), restore or vaulting activities, reboot the Windows system to clear the Windows cache.

▼ Configure a BasicDisk STU

While logged on to the NBU media server as an administrator authorized to run NetBackup, configure the Data Domain system as a BasicDisk STU with the Getting Started wizard or with menu options on the NBU console.

**Note:** This procedure shows use of menu options on the NBU console.

1. In the left window of the NBU console, select Storage > Storage Units > New Storage Unit.

2. Specify the Storage unit parameters.

**Note:** Specify 10 as the maximum number of concurrent jobs (the default value is 1), to allow concurrent jobs to run to this STU.
Figure 6 shows a successfully configured BasicDisk STU with a Data Domain system volume on an NBU media server that runs a UNIX operating system.

![New Storage Unit](image)

**Figure 6:** Basic Disk STU

**Note:** On an NBU media server that runs a Windows operating system, you can specify the absolute pathname to directory with either the Universal Naming Convention (UNC) or the DFS pathname to the Data Domain system. Figure 7 shows an example of a UNC pathname.

![Properties and Server Selection](image)

**Figure 7:** Windows NBU Media Server With a UNC Pathname

3. To configure a CIFS Basic Disk STU on a Windows NBU media server in an AD environment, enter the DFS path name to the Data Domain system.

   Figure 8 shows an example of two DFS links on a DFS Server. In this example, the dd510-1 link contains two targets: `\Dozer\backup` is enabled while `\Dd510-1\backup` is disabled.
Figure 8: Example of Two DFS Links

Figure 9 shows the Absolute pathname to directory that was entered for the DFS link example in Figure 8.

![Figure 9: Absolute Pathname to Directory Example](image)

In the example in a non-production configuration, a backup policy uses the DFS basic disk STU, and the backup destination is the Data Domain system \backup directory. Backups are written to \Dozer\backup because \Dd510-1\backup is disabled.

Caution: In a production environment, carefully consider the infrastructure requirements so you can create the appropriate BasicDisk directory. It is best practice to create additional backup paths on a Data Domain system under \backup for each BasicDisk STU, for example: \Dozer\backup\test.

A successfully configured BasicDisk STU also reflects the properties of the Absolute pathname to directory path.

4. Click Properties in the Change Storage Unit window. The Directory Properties dialog appears as shown in Figure 10.

![Figure 10: Basic Disk STU Properties](image)
VTL STU Configuration

As shown in Figure 11, a Data Domain system configured as a VTL STU is connected to one of the ports on an HBA on the backup software server. The Data Domain system can be connected to the backup software server either directly or through a SAN switch.

![Diagram of Data Domain System Connections for a VTL Configuration]

Figure 11: Data Domain System Connections for a VTL Configuration

▼ Configure a VTL STU

Perform the following procedures to configure a Data Domain system as a VTL STU.

| ▼ Establish the FC Connection and Install Drivers | Page 16 |
| ▼ Create a VTL Group on the Data Domain System | Page 17 |
| ▼ Configure a VTL on the NBU Media Server | Page 17 |
| ▼ Verify Discovery of Media Changers and Tape Devices | Page 19 |

▼ Establish the FC Connection and Install Drivers

1. Physically connect and establish a Fibre Channel (FC) connection between the Data Domain system and the NBU media server.

2. Make sure the correct changer driver and tape driver are installed and loaded on the NBU media server. For the required driver and tape driver refer to the VTL compatibility matrix for the current DD OS release and the Data Domain system model.

3. Log into the Data Domain system as sysadmin, and enter: `vtl initiator show`.

```plaintext
sysadmin# vtl initiator show
```
If the Storage Area Network (SAN) connection is set up correctly, the status of the initiator on the NBU media server host is shown as Online. Figure 12 shows initiators that have been configured with aliases on a Data Domain system.

Figure 12: Initiators With Aliases on a Data Domain System

▲ Create a VTL Group on the Data Domain System

On the Data Domain system, create a VTL group, and add a VTL and the initiator into the VTL group. Refer to the Data Domain Operating System User Guide for 4.5.x for how to set up a VTL.

Figure 13 shows an example of a valid VTL group with one initiator, one changer, and two drives.

Figure 13: A Valid VTL Group With One Initiator, One Changer, and Two Drives

▼ Configure a VTL on the NBU Media Server

1. On the NBU media server, make sure the devices are discovered. Execute the `sgscan` command in the `NetBackup_install_path->volmgr->bin` directory.
Figure 14 shows the discovered devices when the `sgscan` command is entered on an NBU media server that runs a UNIX operating system.

**Figure 14:** Output from `sgscan` Command on an NBU Media Server

2. If the `sgscan` command does not show any tape devices, perform these additional checks.
   a. At the operating system level, check that the medium changer and tape drives are discovered.
   b. At the HBA level, make sure that the LUNs for both the medium changer and tape drives are discovered.
   c. Make sure that the system kernel has enough targets to accommodate the total number of configured tape drives and changer.

See the *Veritas NetBackup 7.0 Device Configuration Guide for UNIX, Windows and Linux* for how to perform the above checks and verifications.

You can see an example of how to configure sg device drivers under Solaris at:

http://seer.entsupport.symantec.com/docs/295572.htm

Refer to the *Veritas Netbackup Device Configuration Guide* to complete the device configuration based on the operating system of the NBU media server.

3. From the NBU console, run the Configure Storage Devices wizard.

4. Select the host that has the Data Domain system VTL attached. Click Next.

   NetBackup auto-detection shows the discovered devices. **Figure 15** shows the devices detected on an NBU media server.

**Figure 15:** NetBackup Media Server Auto-detected Tapes and Robot
5. Complete the steps in the Device Configuration Wizard.

**Verify the VTL STU Configuration**

1. Select the Device Monitor from the left menu of the NBU console.
2. Verify the configuration.

   The Device Monitor shows all configured devices. Figure 16 shows a successfully configured VTL on an NBU media server that runs a UNIX-based operating system.

![Device Monitor](image)

**Figure 16:** Configured VTL Displayed by the Device Monitor

3. Select Storage in the right window of the NBU console.
4. Right click on the VTL STU and select Change.

   Figure 17 shows the properties of a Data Domain system VTL STU. The parameters are default values for a VTL that consist of two tape drives.

**Note:** In Figure 17, multiplexing is not enabled.
**Figure 17:** Data Domain VTL STU

**NDMP STU Configuration**

*Figure 18* shows hardware configuration options for NDMP backups: 3-way NDMP, Local NDMP, and Remote NDMP. *Table 2* defines the options.

**Figure 18:** NDMP Configuration Options
Verify that the NDMP option is installed on the NBU media server. For configuration details, refer to the Veritas NetBackup for NDMP Administrator’s Guide for UNIX, Linux, and Windows.

**Verify NDMP Installation on the NBU Media Server**

1. Go to the `NetBackup_install_path` → `lib` directory.
2. Verify that the `libndmpclient.so` library file exists in the directory.

**Configure an NDMP STU**

1. From the NBU console, run the Configure Storage Devices wizard.
2. Select the NBU media server to configure as the Device Host for NDMP.
3. Click Change. The Change Device Host dialog box appears.
4. Perform the following steps.
   a. Enter a DNS name in the Device Host field. The example shows `z` as the device hostname.
   b. Click the NDMP server checkbox.
   c. Click OK to save the configuration and close the dialog box.
   d. Click Next in the Device Configuration Wizard.

*Figure 19* shows an example of a Device Configuration Wizard and the Change Device Host dialog box configured for NDMP set up.

<table>
<thead>
<tr>
<th>Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local NDMP</td>
<td>The Data Domain system is logically directly connected to an NDMP NAS filer. In <em>[Figure 18]</em> data from NAS filer A is backed up on the locally attached Data Domain system VTL C.</td>
</tr>
<tr>
<td>Remote NDMP</td>
<td>(An NBU term.) Backups can be made from a NDMP NAS filer to a Data Domain system that is directly attached to an NBU media server. In the remote NDMP illustration in <em>[Figure 18]</em> Data Domain system VTL D is attached to an NBU media server; data from NAS filer A is backed up to the Data Domain system VTL D. With Remote NDMP, NDMP type backups and non-NDMP type backups can share the same backup devices that are attached to the media server.</td>
</tr>
<tr>
<td>3-way</td>
<td>Involves two or more NDMP Data Movers and a Data Mover Agent. For example, in <em>[Figure 18]</em> NAS filer B can be backed up to either Data Domain system VTL C or D.</td>
</tr>
</tbody>
</table>
5. Perform the following steps in the NDMP Hosts window.
   a. Click New.
   b. Add the NDMP host and click OK. The New NDMP Host dialog box appears.
6. Configure NDMP credentials.
   Refer to the NetBackup 6.x NDMP Administrator’s Guide for UNIX, Linux, and Windows for details on NDMP Host Credentials. The infrastructure and implementation policy of each site determine the appropriate type of NDMP credentials to configure.
   Figure 20 shows an example of an NDMP host configured to use global NDMP credentials.
7. Follow the wizard steps to complete the NDMP configuration.
8. Verify the settings with the `tpautoconf` command with the `-verify` `-nh` options followed by the name of the NDMP-enabled NAS filer.

```
# tpautoconf -verify -nh ndmp_host_name
```

The following example shows the relevant output of a `tpautoconf` `-verify` command after the host’s NDMP credentials are successfully registered and configured.

Connecting to host "test.new.abc" as user "root"...

...Host info is:
host name "test.new.abc"
os type "NetApp"
os version "NetApp Release 7.x.x.x"
host id "xxxxx"
Login was successful
Host supports LOCAL backup/restore
Host supports 3-way backup/restore

---

**Backup Policy Configuration, Backups and Restores**

A backup policy must be configured before backups can be performed.

**Note:** Because certain required backup policy attributes cannot be configured with the Backup Policy Wizard, the procedure in this section does not use the wizard.

Perform the following tasks to perform backups and restore data on the NBU media server:

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a Backup Policy</td>
<td>23</td>
</tr>
<tr>
<td>Manually Run a Back Up</td>
<td>24</td>
</tr>
<tr>
<td>Restore Backed Up Data</td>
<td>24</td>
</tr>
</tbody>
</table>

▼ **Configure a Backup Policy**

3. Configure the policy as follows for a backup policy to use for backups to a Data Domain system.
   - Verify that Compression is unchecked.
   - Verify that Encryption is unchecked.
   - Specify Take checkpoints every: x minutes when a large volume backup is involved. This allows the backup to restart from the last checkpoint in a case a large volume backup fails for any reason.
• If a VTL STU is being used, verify that Enable multiplexing is not checked. Disabling multiplexing allows a Data Domain system to compress data efficiently.

Note: The Limit jobs per policy setting limits the number of jobs the current backup policy can execute. It limits the number of streams if multiple jobs from the same policy run concurrently, but it does not limit the number of streams per job.

Note: In the Global Attributes that are set from the NBU console under Host Properties, the Maximum jobs per client setting limits the number of jobs that can be set in any policy.

▼ Manually Run a Back Up

1. On the NBU console, select the backup policy.
2. Right click on the backup policy and select Manual Backup.

▼ Restore Backed Up Data

1. From the left menu of the NBU console, select Backup, Archive, and Restore.
2. In the top right of the screen shown in Figure 21, select the hand icon to bring up the Specify NetBackup Machines and Policy Type dialog.

Figure 21: Backup Configuration Icon

3. After configuring machines and the policy to use in the dialog box, click OK.
4. Click the backup history icon to the right of the NBU console to bring up the Backup History dialog.

Figure 22: Backup History Icon

5. In the Backup History Dialog, select the backup to be restored and click OK.
6. Select the files or directories to be restored and click Restore. A Restore Marked Files window appears.

7. Select Destination and Options. Figure 23 shows the selected Destination and Options for a restore example.

![Restore Marked Files Window](image)

**Figure 23:** Selected Destination and Options for a Restore Example

8. Click Start Restore to run the Restore job.

9. Monitor the job from the Activity Monitor.

### Required NetBackup Global Settings

The NBU administrator can choose most parameter settings for the backup policies, STUs, the media server, and the master server host properties based on the needs of the site. The following procedures provide the parameter settings that must be used to enable NetBackup to work with a Data Domain system.

#### Configure Required NetBackup Global Settings

1. On the left menu of the NBU console, select Host Properties.

2. Select Master Servers and select the host on the right pane of the NBU console.

3. Right click to see the drop-down menu and select Properties.

  ![Properties Option](image)

  **Figure 24** shows the Properties option selected from the Master Server pull-down menu.
4. Select Global Attributes and set values that apply to all NBU media servers.

Note: Global Attributes settings on the master server affect all media servers. Consult with your IT department policy to determine which Global Attributes to implement. The default value of the Maximum jobs per client global setting is 1, while Symantec’s recommendation is that the Maximum jobs per client be set at a higher value. Our suggested setting is 10. If a lower value is required for certain storage units, restrict the Limit jobs per policy setting in the backup policies for these STUs.

Figure 25 shows the Global Attributes settings on a test system. In the example, the Maximum jobs per client has been updated to 10.
5. Click OK.


Figure 26 shows the Universal Settings for a master server zee. The Restore retries value allows the NBU administrator to select and implement the retry count for Restore jobs. By default, the value is 0.

Note: The Host Properties settings within NetBackup are robust. Therefore, the NBU administrator can configure the host properties for one master server, media server or client without effects on the other servers or clients in the NBU environment.
Configuration and Use of Logs in Troubleshooting

This section describes how to configure logs and provides an example of how to use logs during a basic debug process.

Log Configuration

When detailed logging is required, consult Symantec’s Support Engineer to determine the correct logging levels to implement for all NetBackup services.

**Caution:** Setting the log levels of any NetBackup services may require NetBackup services to be stopped and restarted. In addition, to enable detailed logging without the proper procedures in place to monitor and remove logs as they accumulate could cause logs to consume all available disk on the system.

Figure 27 shows the default logging parameters for master server zee.

![Figure 27: Default Logging Parameters for NBU Master Server zee](image)

A NetBackup 6.x system has two types of logs: unified logs and the legacy NetBackup logs.

- Unified logs are located in `NetBackup_install_path → logs → directory`. Refer to the Symantec Veritas NetBackup 6.x Troubleshooting Guide for Unix and Windows on how to use the `vxlogview` command to view NetBackup’s Unified logging entries. You can obtain NetBackup examples of viewing unified log entries from: [http://seer.entsupport.symantec.com/docs/278059.htm](http://seer.entsupport.symantec.com/docs/278059.htm)

- Legacy logs are located in `NetBackup_install_path → netbackup → logs directory`. Run the `mklogdir` command to create the legacy log folders.

The following procedures describe how to configure the logs, view unified logs, and provide a basic example of how to use the logs in troubleshooting.
Note: Not all NetBackup/Data Domain integration issues are as simple to debug as the one shown in the example. The example shows logical steps for review of NBU logs, but the example may not replace the need for Data Domain engineering analysis or the support of Symantec TSA net.

▼ Configure Logging

1. From the left menu of the NBU console, select Host Properties.
2. Select Master Servers and select the host on the right pane of the NBU console.
3. Right click to see the drop-down menu and select Properties.
4. Select Logging and tune the logging parameters as desired.

▼ View Unified Logs

1. Go to the NetBackup_install_path → netbackup → bin directory.
   
   ```
   # cd NetBackup_install_path/netbackup/bin
   ```

2. Enter the vxlogview command with the following options:
   
   ```
   vxlogview -p 51216 -X jobid=N > N.log
   ```
   
   In the following example, the job ID is 1. The redirect (>) pipes the log results to an output file named 1.log for debugging purposes.
   
   ```
   # vxlogview -p 51216 -X jobid=1 > 1.log
   ```

▼ Debug a NBU Failed Job (Example)

1. Select the Job Details for the failed job and find out when the first error occurred.

   Figure 28 shows Job Details for a failed backup. The Status field on the Job Overview tab indicates the job failed with media write error(84).
2. Select the Detailed Status tab and look for the plugin error.

The Detailed Status tab shows excerpts from the bptm.log file. The first error message (highlighted in Figure 29) is **Critical bptm(pid=884) image write failed with a plugin error.**

**Figure 28:** Job Details for a Failed Job

**Figure 29:** Detailed Status Example
3. Review the bpdm.log.

The example excerpt from the bpdm.log file shows that the backup failed because OST is not enabled.

```
15:57:48.984 [324.296] <16> dd510-1.support.datadomain.local: C:\Program Files\Veritas\NetBackup\bin\ost-plugins\libostspi DataDomain.dll:stspi_get_server_prop STS_EPLUGIN ost get property failed: not enabled (nfs: Permission denied)
```

Resolution of an NBU Resource Request Failure

In a Windows environment, backups to BasicDisk STUs can fail with NBU status 800 “resource request failed” after an upgrade to NetBackup 7.0. If this error occurs, perform the following procedure. See Symantec’s support document ID 295201 at: http://seer.entsupport.symantec.com/docs/295201.htm for details.

▼ Resolve Failure After NBU 7.0 Upgrade on Windows

Perform the following steps if NBU status 800 “resource request failed” error occurs after an upgrade to NetBackup 7.0.

1. Change the logon accounts for the following services:
   - Netbackup Remote Manager and Monitor Service
   - Symantec Private Branch Exchange
   - Netbackup Client Service

2. Restart the NetBackup services to put the changes into effect.

Performance Tuning

**Advanced Topics**

This section covers the following advanced topics.

<table>
<thead>
<tr>
<th>“NetBackup SSO Configuration” on page 32</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Data Domain Replication Configuration and Restoration” on page 33</td>
</tr>
<tr>
<td>“Restoration of VTL Volumes from a Replica” on page 33</td>
</tr>
</tbody>
</table>

**NetBackup SSO Configuration**

Shared Storage Option (SSO) is a NetBackup feature that allows tape drives to be shared between multiple NBU media servers. When you set up SSO, make sure all NBU media servers are within the same SAN zone. Figure 30 shows an example configuration of a Data Domain VTL with one NBU master server and two NBU media servers that are connected to a SAN switch. On the SAN switch, the NBU media servers are zoned with the same Data Domain system VTL.

![NetBackup SSO Configuration With a Data Domain VTL](image)

**Figure 30:** NBU SSO Configuration With a Data Domain VTL

**Set Up an SSO Configuration**

Following are the basic requirements for an SSO set up.

1. Make sure an NBU SSO license is installed on the NBU master server and on all the NBU media servers that share the VTL.
2. Verify that the correct tape device and changer drivers are loaded for all the platforms.
3. Verify that all the media servers detect the VTL and the tape drives that are going to be set up for SSO.
Figure 31 shows how a Data Domain system VTL that is shared in the SSO environment is presented from the NBU console’s Media and Device Management window.

For Veritas-recommended device configuration techniques and troubleshooting tips for tape library configuration, see the *Veritas 7.0 NetBackup Device Configuration Guide*.

**Data Domain Replication Configuration and Restoration**

Data Domain replication types are collection replication and directory replication.

- Collection replication replicates the complete `/backup` directory from one Data Domain system to another Data Domain system.
- Directory replication is more granular. It allows for replication at the individual directory level.

**Restoration of VTL Volumes from a Replica**

To restore backups from VTL volumes from a Data Domain system replica, existing volumes in the current VTL must be exported out of the current VTL library. In a physical tape library, the physical tape volume is exported out from one physical tape library, moved and imported into another physical tape library. With VTL the export and import processes are non-physical. Virtual tape volumes that are exported out of a VTL tape library are put into a virtual vault. Figure 32 shows virtual tape volumes that are now in the vault location.
Once the volumes are exported to the vault, the volumes that were replicated to the secondary Data Domain system must then be imported into the new VTL library.

**Restoration of a Replica Configured as a BasicDisk STU**

Restore from a Data Domain system replica configured as a BasicDisk STU is not straightforward because NBU does not know that replication has taken place and that an alternative device is available. The following is an example of how to execute a restore from a Data Domain system replica from the same Solaris NBU media server.

**Figure 33** shows the Absolute pathname to directory for the STU basicDisk_dd510 is /mnt4/test. **Figure 34** shows dd510-1:/backup is mounted on /mnt4.
Figure 33: STU basicDisk_dd510 With /mnt4/test Backup Destination

Figure 34: dd510-1:/backup Mounted to /mnt4

Figure 35 shows that STORAGE_GRP contains basicDisk_dd510 STU.
Figure 35: STORAGE_GRP Contains basicDisk_dd510 STU
Figure 36 shows NetBackup backup policy zee uses the Storage Group STORAGE_GRP which contains the basicDisk_dd510 STU.

Figure 36: Backup Policy zee With STORAGE_GRP as the Policy Storage
Backup policy zee is executed and backup completes successfully with the STORAGE_GRP policy.
Configure Replication and Restore from a Replica

Replication configuration procedures are listed in the following table.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Replication on the Data Domain System</td>
<td>37</td>
</tr>
<tr>
<td>Import Volumes Into a New VTL Library</td>
<td>37</td>
</tr>
<tr>
<td>Restore a VTL from a Secondary Data Domain System</td>
<td>38</td>
</tr>
<tr>
<td>Restore from a Replica Data Domain System</td>
<td>38</td>
</tr>
<tr>
<td>Restore from a Secondary Data Domain System</td>
<td>39</td>
</tr>
</tbody>
</table>

Configure Replication on the Data Domain System

1. Log into a Data Domain Enterprise Manager Web console.
2. Verify that the replication license exists.
3. Configure replication as described in the *Data Domain Operating System User Guide*.

Figure 37 shows an example of directory replication on a Data Domain system. In the example, the source (primary Data Domain system) is dozer.d.d.l, the destination (secondary Data Domain system) is dd510-1.

![Figure 37: Directory Replication on a Data Domain System](image)

Import Volumes Into a New VTL Library

On the command line of the secondary Data Domain system, run the `vtl import` command with the following syntax:

```
vtl import vtl_name barcode barcode [count count] [pool pool_name] [element drive | cap | slot] [address addr]
```

Figure 38 shows replicated VTL tape volumes from the secondary Data Domain system that have been imported into the new tape library named vtl.

![Figure 38: Replicated VTL Tape Volumes](image)
Figure 38: Replicated VTL Tape Volumes in the vtl Tape Library

▼ Restore a VTL from a Secondary Data Domain System

1. Export the VTL tape volume(s) from the current VTL. Use NetBackup to export the volume(s). For example, export BBB000 volume from NBU.

2. From the current DDR, execute `vtl export` to export the volume(s) to the vault location with the following syntax:

   ```
   vtl export vtl slot address count count
   ```

3. From the replica DDR, execute `vtl import`, to import the volume(s) into the replica VTL with the following syntax:

   ```
   vtl import vtl barcode barcode
   ```

   ```bash
   sysadmin#dd510-1# vtl import vtl2 barcode BBB000
   ```

4. Execute a NetBackup inventory to update the replica VTL with the imported volumes.

5. Backup images, can be recovered from the write-protected replica VTL volume.

▼ Restore from a Replica Data Domain System

1. Before you attempt to restore from a replica Data Domain system, verify that Data Domain replication has been sync-ed. For example, the `df -k` command output on a UNIX media server in Figure 39 shows that `/mnt4` has been remounted with the secondary Data Domain system path.
2. Execute a restore of the backed up image. Figure 40 shows a successful restore of a backup from the secondary Data Domain system from the same Solaris NBU media server.

**Figure 39:** /mnt4 Remounted With the Secondary Data Domain System

**Figure 40:** Restore from a Secondary Data Domain System

**Restore from a Secondary Data Domain System**

This procedure describes how to restore from a secondary Data Domain system connected to a different NBU media server. The mount point is shown as /mnt4 in the examples of how to mount the secondary Data Domain system on the NBU media server #2. The NBU commands swap the backup image for restore from a different server.
1. Go to the *NetBackup_install_path → netbackup → bin → admincmd* directory.

2. Execute the command `bpimagelist -L` to view the backed up images.

3. Identify the backup image to be restored. For example, Figure 41 identifies an image to be restored.

4. Specify the image to be restored from the second media server. Run the `bpimage` command with the following syntax:

   ```bash
   bpimage -newserver new_server_address -oldserver old_server_address -id image_filename
   ```

   **Note:** The image file specified with the `-id` option must be available for restore from the second media server.

   The following example specifies that the backup image `zee_121926335_C1_F1` should be restored from `media_server2.test.local` instead of `media_server1.test.local`.

   ```bash
   # bash-3.00# bpimage -newserver media_server2.test.local -oldserver media_server1.test.local -id zee_121926335_C1_F1
   ```

**Figure 41:** Backed up Image Identified by the Backup ID